Security in Information Systems :

The identification of risks in selected electronic banking applications

A thesis presented in partial fulfilment
of the requirements for the degree of

Master of Business Studies in Information Systems

at

Massey University

Elizabeth A. Kemp

February, 1988

Acknowledgements

In presenting this thesis, I would like to take the opportunity to express my thanks to the following people for their help and support :

Firstly, my supervisor, Richard Hayward, for his guidance, criticism and encouragement throughout the course of the project.

Secondly, Professor Rae Weston for her invaluable suggestions and comments about security issues in banking.

Finally, I would like to thank my family, Raymond, Rebecca and Stephen, for all the support they have given me in so many ways during the completion of this thesis.

Abstract

This thesis considers the security threats associated with the introduction of electronic banking. In electronic banking services the paper based instructions for the movement of money are replaced by the electronic transmission of data. Since electronic banking relies heavily on advanced information technology (the use of computers and communications), security is a matter of grave concern. This thesis identifies the principle risks to security in five electronic applications : Automated Teller Machines (ATMs), Electronic Funds Transfer, Point-of-Sale (EFTPOS), credit cards, home banking and wire transfers. Both the information technology used and the applications are described. The major threats to each element of the computer system, hardware, software, data, communications and the environment are identified and related to the appropriate service. Five major risk categories are described : disaster, accident, error, computer abuse and sabotage. These headings are used as the starting point for the analysis of risks to each component of the system.

Table of Contents

Chapter 1 Introduction 1
1.1 The banking industry and information technology 1
1.2 Scope of the thesis 4

Chapter 2 Computer Security 7
2.1 Introduction 7
2.2 The security problem 7
2.3 Risk management 17

Chapter 3 The Use of Computers in Banking 19
3.1 Introduction 19
3.2 Hardware 19
3.3 Data 20
3.4 Communications 22
3.5 Software 34
3.6 Cards 37
3.7 Personal Identification Number (PIN) 42
3.8 Conclusion 44

Chapter 4 A Description of the Electronic Banking Applications 45
4.1 Introduction 45
4.2 Automated Teller Machines 45
4.3 EFTPOS 58
4.4 Credit cards 70
4.5 Home banking 78
4.6 Wire Transfers 88

Chapter 5 Threats to Hardware 99
5.1 Introduction 100
5.2 Disaster to hardware 100
5.3 Accident 102
5.4 Error 103
5.5 Computer abuse 104
5.6 Sabotage 106
5.7 Conclusion 108

Chapter 6 Threats to Software 110
6.1 Introduction 111
6.2 Disaster 111
6.3 Accident 111
6.4 Error 112
6.5 Computer abuse 118
6.6 Sabotage 127
6.7 Conclusion 128

Chapter 7 Threats to Data 129
7.1 Introduction 130
7.2 Disaster 130
7.3 Accident 131
7.4 Errors 131
7.5 Computer abuse 142
7.6 Sabotage 171
7.7 Conclusion 171

Chapter 8 Threats to Communications 173
8.1 Introduction 174
8.2 Disaster 174
8.3 Accident 174
8.4 Errors 176
8.5 Computer abuse 179
8.6 Sabotage 187
8.7 Risks to encryption and message authentication 188
8.8 Conclusion 197

Chapter 9 Threats to the Environment and Organisation 198
9.1 Introduction 199
9.2 Disaster 199
9.3 Accident 199
9.4 Error 199
9.5 Computer Abuse 203
9.6 Sabotage 207
9.7 Organisational issues 207
9.8 Conclusion 219

Chapter 10 Conclusion 220
10.1 Introduction 220
10.2 Key risks 221
10.3 Countermeasures 223
10.4 Summary 225

Appendix 1 Discovery of a PIN 227

Appendix 2 Glossary 235

Bibliography 239

Figures

Figure 2.1	Sensitive applications (Lane,1985)	11
Figure 2.2	Risk identification model	18
Figure 3.1	Network Components	22
Figure 3.2	Single Processor Sharing (Orkand Corporation,1983)	26
Figure 3.3	Front-end Switch (Orkand Corporation,1983)	26
Figure 3.4	Back-end Switch (Orkand Corporation,1983)	26
Figure 3.5	Local area controller	27
Figure 3.6	MAC Processing (ANSI X9.9,1982)	33
Figure 3.7	Communications Software (Ritchie,1987)	36
Figure 3.8	Magnetic stripe card	38
Figure 3.9	Smart card (McIvor,1985)	40
Figure 4.1	ATM keyboard	46
Figure 4.2	Off-line ATM (Orkand Corporation,1983)	48
Figure 4.3	On-line ATM (Orkand Corporation,1983)	49
Figure 4.4	ATM Network	49
Figure 4.5	Front-end ATM network	50
Figure 4.6	Back-end ATM network	51
Figure 4.7	EFTPOS system (Lipis,1985)	59
Figure 4.8	On-line EFTPOS with smart card (Brown and Brown,1986)	62
Figure 4.9	Back-end EFTPOS system	63
Figure 4.10	Open Access system	64
Figure 4.11	Front-end EFTPOS system	65
Figure 4.12	Store and forward system (Brown and Brown,1986)	73
Figure 4.13	Videotex system	80
Figure 4.14	Home Banking System	83
Figure 4.15	Wire transfer system (Lipis,1985)	89
Figure 4.16	Domestic wire transfer (Lipis,1985)	90

Figure 4.17	International wire transfer (Lipis,1985)	92
Figure 5.1	Hardware	99
Figure 6.1	Software	110
Figure 7.1	Data	129
Figure 8.1	Communications	173
Figure 9.1	Environment and the organisation	198

Tables

4.1	Principle risks in all ATM systems	54
4.2	Additional risks in off-line systems	56
4.3	Additional risks in on-line systems	57
4.4	Principle risks in EFTPOS systems	67
4.5	Principle risks in all credit card systems	74
4.6	Additional risks to magnetic stripe cards	77
4.7	Additional risks to smart cards	77
4.8	Principle risks in home banking systems	85
4.9	Principle risks in wire transfer systems	96
9.1	Cap Information (Cline,1986)	211

Chapter 1

Introduction

1.1 The banking industry and information technology

With the introduction by the finance industry of applications based on advanced information technology (the use of computers and communications), it has become apparent that the security of such systems is a matter of grave concern. Both banks and customers stand to lose from the weaknesses endemic in the technology. The purpose of this thesis is to identify the principle risks to security in five applications that are central to electronic banking: Automated Teller Machines (ATMs), Electronic Funds Transfer, Point-of-Sale (EFTPOS), credit cards, home banking and wire transfers. Both the information technology used and the applications are described. The major threats to hardware, software, data, communications and the environment are then analysed in terms of the principle risks : disaster, accident, error, crime and sabotage.

In the past few years financial institutions all over the world have chosen to offer a wide range of services to their customers that depend upon computing technology. These include Automated Teller Machines (ATMs), bank credit and debit cards, Electronic Funds Transfer Point-of-Sale services (EFTPOS), Automated Clearing House Services, home banking, cash management and wire transfers. Not all of these are new services, wire transfers, for example, but in their present form they all rely heavily on computing technology. These services are often referred to as electronic funds transfer (EFT) applications since paper based instructions for the movement of money are replaced by the electronic transmission of such data. A more meaningful term also used to describe such services is electronic banking. This seems more appropriate than electronic funds transfer in the present climate where banks deliver not only money but also financial information and transaction services to the customer as required. Banks, therefore, have become very dependent upon the entry of data and its manipulation by the computer since it represents both information and money.

Various factors have led to this expansion of services. Bankers themselves identified three principle forces that currently shape payment systems, technology, cost revenue relations and competition (De Mattia, 1985). Computer technology and associated advances in telecommunications make it possible for banks to transfer and act upon messages from their customers very quickly. Payments made at the point of sale as well as small incoming and outgoing payments can easily be automated. Banks can also process and settle high value payments in one day. The use of computer technology to add value to products and services has become widespread. The large and sophisticated systems needed to support such processing can be developed using an effective information systems strategy which enables an organisation to plan its application, technology and management policies to achieve its business goals. The costs associated with such a system are rapidly decreasing; the reduction in the price of hardware (mainframes and terminals) as well as cheap rates for data transmission on packet-switching networks have made possible great economies in scale.

Cost revenue relations have become particularly important in view of two developments. In the first place banks need to replace their lowered profits from interest income by earning fees from the various services that they offer their customers. Retail banks have found that lending out the deposits has proved less and less profitable as the competitive environment has had the effect of significantly increasing the cost of collecting the deposits in the first place. These costs are difficult to recoup so there has to be some means of reducing operating costs (Bailey,1986). Secondly, bank payment systems throughout the world are having to handle an increasing numbers of cheques. There appears, unfortunately, for the banks, to be a trend to use cheques for lower value payments (Read,1983). Replacing the cumbersome and relatively costly processing of cheques by alternative services such as ATMs and EFTPOS should help reduce costs for the banks. Figures provided by Lipis (1985) indicate that the cost of a teller transaction is well above the average ATM transaction cost.

Various competitive forces have compelled banks to making increasing use of information technology. Financial deregulation in many countries of the world has made it possible for non-banks to carry out functions once the sole prerogative of banks. These institutions have been able to make use of this opportunity because of the lowered barriers to entry. Technological changes mean that there is no longer any necessity, for example, to have a large number of branch outlets in order to meet the needs of the customer effectively. In order to survive banks have to use the same technology as their competitors. Their reasons for providing an attractive range of services include all or some of the following : generating new and profitable accounts, higher retention of present accounts, enhanced image of the organisation, competitive advantage and expansion of geographic coverage at considerably less cost than traditional branch activities (Bennet,1976). It is not only on the domestic front that banks have to act. The internationalisation of the finance industry is another reason why banks have had to adapt their competitive strategies. With a system of international markets, increasing trade between the subsidiaries of transnational corporations and an international spread of corporate related services, the banks are having to integrate their operations on a global basis (Langdale,1985). Again, it is computer technology that makes this possible.

Banks are currently in a transitional phase. Once they held a legal monopoly on the payment system, now they have been forced to respond to economic and technological forces to ensure their survival. They have done this by making available electronic banking services that are offered off-premises as well as on. A survey carried out by Louis Harris and Associates (1985) on behalf of Coopers and Lybrand revealed that most of the large banks which offered these technology-enhanced or technology-dependent products believed that these applications were on the "cutting edge", that is relatively new and untried. They felt committed to such a course of action in order to keep up with the competition. The speed at which changes have been introduced is causing some concern not least from a security point of view. As early as 1983, Miller noted that "with the concentration of more and more operating functions in computer systems, characteristics

of threats change, exposures to loss increase greatly." He listed nineteen possible exposures that could result from a threat, the principle of which are loss of assets, the cost of litigation, the loss of business and increased insurance fees.

Banks not only have to worry about the financial losses they could sustain but are also particularly vulnerable to a loss of confidence on the part of their customers. Any threat to their reputation can lead to a "run-on the bank" by their customers, resulting very quickly in bankruptcy. In order to avoid such a contingency and to minimize monetary losses, many banks have instituted a risk management programme. The first stage of this process provides for the identification of threats to security. Once this has been carried out, a bank can decide how much to spend on measures to reduce the risks. Both the likelihood of a threat materialising and the consequent losses have to be taken into account. If the risk management procedure is carried out properly management can reduce the overall level of risk in the system. Moreover, substantial savings in insurance costs can be achieved since premiums are related to the effectiveness of the controls in place. At a time when insurance fees are rising rapidly, this gives financial institutions a great incentive to make a realistic appraisal of weaknesses in the services they offer and implement suitable controls. The most important stage in this exercise is the initial identification of the principle risks.

1.2 Scope of the thesis

The author is unaware of a comprehensive survey of risks associated with the introduction of electronic banking. This study attempts to address this by identifying the major security risks in five important applications. At a time when more and more financial institutions are bringing technology-dependent products on to the market, it is important to analyse the applications in order to determine the major security threats. This should prove helpful not only to those working in this area but also to the general public whose interests have to be safeguarded. The scope of the study is limited to five electronic banking services : Automated Teller Machines, Electronic Funds Transfer Point-of-Sale,

bank credit cards, home banking and wire transfer systems. The first four of these are applications that are currently or, banks would like like to see, well-patronised by the general public. Wire transfer systems, on the other hand, are more often used by corporations. They involve the movement of huge sums of money daily and are crucial to the economies of the west. Whether the application is a matter of private or public interest, however, customer and bank monies are at risk. The five applications selected are described in some detail prior to the analysis of risks. This is an integral part of the thesis since the risks identified have to be related to a specific environment.

The principle risks consequent upon the use of computer technology are identified and described. Real-world examples, taken mainly but not solely from the banking industry, are included to illustrate the dangers. Each application is not the subject of a separate chapter since this would involve a great deal of duplication. Many risks (for example fire at a computer installation) are common to all the electronic banking services. Instead, the threats to each element of the computer system : hardware, software, data, communications and environment, are identified and related to the appropriate service.

Five major risk categories have been identified from the study of the literature : disaster, accident, error, computer abuse and sabotage. These are used as the starting point for the analysis of the risks to each component of the system. A threat can be seen from many perspectives. To take an example, a transaction can be altered when transmitted along communication lines. This is classified as the unauthorised modification of data in chapter 7 but as an active wire tap in chapter 8. It is essential to view an action from these different angles. Not only does this approach provide a double check so that no major risk is overlooked but makes it easier to provide appropriate solutions as it often identifies the method of attack. Finally, many risks arise from a combination of circumstances and have to be categorised in more than one place.

There are three sources for the material in this thesis; firstly published material, the books and articles written by security professionals, handbooks published by banking organisations, international and national standards, working documents of organisations involved with setting up banking applications and press reports (including the electronic mail journal "Risks-List"); secondly, discussions with EDP auditors, data security staff and university colleagues to clarify the issues involved; lastly, the application of the principles derived from the previous two sources.

The structure of the thesis is as follows:

Chapter 2

An introduction to the problem of security in computer systems with a discussion of the model that has been used as the basis of risk analysis.

Chapter 3

A description of the technology used in electronic banking

Chapter 4

A description of the electronic banking applications selected. Sufficient detail is given to enable examples in the body of the text to be comprehensible.

Chapter 5

The risks associated with hardware

Chapter 6

The risks associated with software

Chapter 7

The risks associated with data

Chapter 8

The risks associated with communications

Chapter 9

The risks associated with the environment

Chapter 10

This chapter contains the conclusion

Chapter 2

Computer Security

2.1 Introduction

In this chapter attention is focussed on the problem of security in computer systems, a definition of "security" is given, factors which exacerbate the security problem are outlined, and the potential costs of security failure are examined. Both the elements of the computer system in need of protection and the risks faced are identified and described. Finally, a risk management methodology is discussed and a model for the identification of risks described.

2.2 The security problem

The information generated by computer systems is vital not only to the day-to-day running of an organisation but also to planning for the future. This increasing dependence on computer technology has made the information assets of an organisation highly vulnerable. Security is concerned with protecting computer-based systems from fire, fraud or any other occurrence that may adversely affect an organisation. If an event of this kind occurs then a breach of security is said to have taken place and, as a result, a loss of some nature may be sustained. It is to avoid such losses that security measures are put in place. The main dangers (Norman,1983), (Pritchard,1978) are seen as:

1. loss of integrity, the data is not accurate, complete and reliable
2. loss of availability of service, the service required cannot be provided within a suitable time period
3. loss of confidentiality, information has been obtained by those who should not have access to it.

Any of these can occur either by accident or design. A comprehensive definition of security which takes into consideration all of these points is given by Lane (1985).

Security - The protection of data from accidental or deliberate threats which might cause unauthorised modification, disclosure or destruction of the data; and the protection of the information system from degradation or non-availability of service.

Consequently, those responsible for security have to minimise the risks associated with the use of the computer. The policies and operating procedures implemented need to be cost effective, however, since an unlimited amount of money can be spent on security without any guarantee of commensurate protection. Finally, those responsible for security in an organisation have to be aware that each step forward using new technology may have serious implications for security.

2.2.1 Magnitude of the security problem

Since the information stored in computer systems is now seen as an important resource, its protection is a matter of great concern (Drucker,1964). The following factors have significantly aggravated the security problem :

1. Computer accessibility is no longer restricted to the computer room : dial-up facilities are available and these reduce the effectiveness of physical controls. As Goldstone (1985) observes of telecommunications, "Their use has the effect of extending the geography of the security concern."
2. Computer usage in organisations has significantly increased as computers have become cheaper and more powerful.
3. User access to data is greatly increased by the provision of database software, fourth generation languages and advanced communication networks
4. The computer literacy of the general public has greatly increased with the advent of microcomputers.

2.2.2 Costs associated with a security failure

Once a breach of security has occurred, the financial costs have to be calculated. These may be so great that an organisation can no longer function. Various costs may be incurred:

1. The cost of fraud when either money or goods have been taken.
2. The cost of replacing stolen hardware or communications equipment.
3. The cost of recreating data that has been lost or modified as a result of either a natural disaster or unauthorised procedures.
4. Legal costs that may arise from the use of incorrect data or the failure to process data correctly
5. The loss of revenue incurred through the inability to process data or by the unauthorised disclosure of proprietary information.
6. Payments made in error because of lack of controls in the system.
7. The loss of business confidence in an organisation.

2.2.3 The security environment.

In order to avoid any or all of the costs outlined above, the various components of the computer system need to be protected. These can be classified as hardware, communications, data, software and the environment. Each of these will be described briefly so that the nature of the security problem can be seen more clearly.

2.2.3.1 Hardware

Hardware refers to the physical equipment which supports the processing of data and includes not only the computer with its main memory and central processing unit but peripherals such as tapes, disks, magnetic drums, printers, plotters and terminals. In the 1970s the hardware would have been limited to a mainframe computer at a single site with card readers, printer, control console and secondary storage. Nowadays, whilst firms might still own or lease a mainframe, both minicomputers and microcomputers are likely

to be widely used. Indeed, as computers have become simultaneously smaller and more powerful, the figures for sales of microcomputers have risen dramatically.

2.2.3.2 Software

Systems software, operating systems, compilers, translators, pre-processors, linkage editors, and application programs are all vulnerable. Large sums of money are invested in the purchase or development of programs all of which require the same degree of protection as data. In the case of systems software, it is essential that this be kept secure from interference in order to ensure the effective functioning of the computer system. Applications software is equally important since it has to process the data that has been collected by the organisation. Obviously application programs and the associated data are mutually dependent, the information generated will be incorrect when either one or the other is erroneous. The scope of the problem is shown by Lane (1985) in figure 2.1 which shows both the wide range of applications and their data to be protected together with the appropriate security objective.

2.2.3.3 Data

Data in a computer based system is at risk whether resident on secondary storage, being processed by a CPU or transmitted along communications lines. Yet it is now considered as an asset equal in importance to cash and inventory. John Opel (Buurmeijer,1984) of IBM says.

> Next to our people, no assets are of greater value than the information we generate in our business. Physical assets are replaceable, proprietary information is not.

An organisation's dependence on data is also increased by the fact that the other assets of an organisation are also represented by data in a computer system. Data can be stored on backing devices such as tape and disk at a very high density in a small physical space and retrieved at speeds hardly imaginable to the human mind - nanoseconds and picoseconds (billionths and trillionths of a second). Since this data cannot be" seen" there are no

Type of Application	Examples	Security Objective
Accounting	Purchases accounting Sales accounting Payroll Stock control	Data integrity
General computer processing	Scheduling of plant maintenance Simulation of wider distribution network CAD	Data integrity
Automated decision making	Reordering of stock Automated payments	Meticulous data integrity
Management information	Centralised MIS Centralised databases	Data confidentality and integrity
Real-time control	City road traffice control Air traffic control Factory automated production control	Continual availability of computer processing and meticulous data integrity
Corporate and national systems	Electronic funds transfer Nuclear materials control National security Car manufacturer's new design	Meticulous data confidentiality and integrity (perhaps with continual processing capability)

Figure 2.1 Sensitive applications (Lane,1985)

obvious signs when data is altered, retrieved or deleted either accidentally by a staff member or deliberately by an individual not authorised to do so.

2.2.3.4 Communications

Distributed computing with the dispersal of services to users has become commonplace. The components of the system are sited at many locations and need to be connected together for the transmission of data to and from the host computer. Both wide area networks (WANs) and local area networks (LANs) may be used. A wide area network is provided by a common carrier or a private organisation either nationally or internationally, whereas a local area network is generally set up by a firm within a geographically limited area such as a building or group of buildings. Again equipment has to be protected, in this case communications controllers, front end processors, multiplexers and modems. Transmission media also have to be considered. Many types of links are available, coaxial lines, fibre-optic cables, twisted-pairs, telephone lines, microwave and satellite.

2.2.3.5 Environmental and organisational issues

Pritchard (1978) classifies the environment as one of the assets in a computer system that must be safeguarded. By the environment he means support facilities such as the air conditioning plant, waste disposal and drainage. Whilst this may seem an unusual classification, it becomes obvious on reflection that sabotaging the air conditioning, for instance, can cause as much damage as a more direct attack on computer hardware. Moreover, in electronic banking, where many services are now offered outside of bank premises, the location of terminals and ATMs is of considerable concern. Finally, this thesis considers briefly other issues of concern to an organisation related to the introduction of computer based technology such the resolution of disputes between banks and their customers.

2.2.4 Classification of threats

Events that can lead to a breach of security are generally known as threats or risks. No comprehensive list of all the threats to computer based systems can be given since the possibilities are infinite with both accidental and deliberate events responsible for a loss of integrity, confidentiality or timeliness in computer-based systems. The types of risk can be broadly classified, however, and this simplifies the process of identifying the principle security exposures in a system. Different writers have all developed their own framework. Martin (1973) states that the major threats are Acts of God, hardware and program failures, human carelessness, malicious damage, crime and the invasion of privacy. A briefer list is given by Mair, Wood and Davis (1978) : human errors, hardware/software failures, computer abuse and catastrophe. Lane (1985) sees the generic threats as the malicious acts of people, external disaster and system reliability.

The following classification of threats will be used in this thesis : disaster, error, accident, computer abuse and sabotage. Disaster and error are universally recognized as risks even if different terminology is used by those working in the area. The accident category is necessary to distinguish events that cannot be classified as disasters but have something of the same impact on a smaller scale. An unreadable disk would be an example of this. Computer abuse, ranging from fraud to the activities of hackers, is a universally accepted problem and is of increasing concern to organisations. Sabotage or malicious damage needs to be looked at separately from computer crime because, although unlawful, it is not committed for any private gain. This activity can only be guarded against if its random nature is comprehended; it is of the essence of sabotage that unexplained or seemingly pointless acts are carried out. This classification of threats makes the important distinction between accidental and deliberate events. The first three threat categories, disaster, error and accident, all happen by chance whilst the other two, computer abuse and sabotage, are deliberate acts.

2.2.4.1 Disaster

Catastrophes may be responsible for causing havoc in computer installations. Martin (1973) mentions fire, flood, Act of War, chance and totally unforeseen events as the causes of large scale damage. Whatever the disaster, the consequences are usually serious for the availability of services and the integrity of data. Fire is the single greatest hazard that has to be faced, followed by flood. These events do not occur very often but power cuts are not infrequent and have to be taken as seriously as the other two threats. Furthermore, totally unforeseen events can be devastating since no preventive planning is possible. Lastly, the above hazards cannot, in real life, be neatly separated; flooding of an installation, for instance, can be the result of fighting a fire.

2.2.4.2 Error

Human error is responsible for more losses than computer crime. Martin (1973) observes "there have been innumerable stories in the press about computers making monumental and often comic errors". Of course, generally speaking, it is not the computers but people at fault. Perry (1981) lists several problems that the human element introduces :

1. The improper use of technology : losses are caused by the failure to use technology properly.
2. The cascading of errors : one error causes another error and so on.
3. Illogical processing : losses are associated with unusual processing that most people would detect as an error. For example a payroll cheque for $1 million would be seen as incorrect if people were processing the data.
4. Repetition of errors : losses are associated with programs following the same erroneous logic on every transaction of that type.
5. Incorrect entry of data : losses are associated with translating data to machine-readable media.
6. Incorrect use and interpretation of data : losses are associated with users of computer data making bad business decisions due to misunderstandings of the accuracy, completeness, consistency, or timeliness of data.

2.2.4.3 Accident

This threat can be distinguished from a disaster by the magnitude of the event. In the case of a disaster the major part of a system is likely to be affected whereas with an accident one component may be damaged. Some examples of the latter include an unreadable disk, a tape that has been damaged by a tape unit or a group of terminals that becomes unusable after the cable connecting them to the computer is cut by workmen putting in power lines. The consequences of such incidents can still be serious and it is statistically more likely that an organisation will suffer from accidents like these rather than a major disaster. Suitable measures have to be taken, the most important of which is the regular backing up of data and software, including that held on personal computers.

2.2.4.4 Computer abuse

Computer abuse, computer crime and computer fraud are all used in the literature to describe those unlawful acts that involve the computer directly or indirectly (Martin,1973), (Parker,1976), (Krauss and MacGahan,1979). Krauss observes that people who commit computer-assisted crimes generally use the computer either directly or as a vehicle for deliberate misrepresentation or deception. This is often to cover up the embezzlement or theft of money, goods, services or information. Many crimes have been described by various authors; these can be grouped into the following categories (Krauss and MacGahan,1979), (Fernandez,Summers and Wood,1981).

1. Theft of money in all forms.
2. Theft of merchandise and inventory of all types.
3. Misappropriation of computer time or stealing computer resources.
4. Theft of data and software.
5. Misrepresentation for financial, personal and political advantage.

There is also a group of people who cannot resist the intellectual challenge of breaking through the barriers that have been set up to protect computer systems. Often teenagers, these hackers with a personal computer and a modem are easily able to make use of the computer and telephone networks that in many developed nations link banks, universities, corporations and government installations. Organisations obviously have to take the threat of hackers seriously and be prepared to deal with these technological whizz kids.

The term "hacker" was coined specifically by the computer industry. Other terminology used in the literature to describe people attacking computer systems include enemy, opponent and perpetrator in addition to the more obvious criminal and saboteur (Krauss and MacGahan,1979), (Davies and Price,1984).

2.2.4.5 Sabotage

Deliberate attempts to damage hardware, communications, software and/or data can be described as sabotage. These malicious activities may occur on a large or small scale. They can be carried out either by complete outsiders or by members of an organisation's staff. In Italy bombing and arson were among the favourite methods of Red Brigade terrorists. Malicious damage by disgruntled employees can also have serious consequences. Martin (1973) mentions several cases ranging from a dissatisfied employer erasing every file and program that his company possessed to computer maintenance staff on strike who sabotaged an insurance company's teleprocessing system. By its very nature, sabotage is difficult to guard against. It is impossible to prevent all acts of this type from occurring, even an apparent accident like the spilling of coffee over a microcomputer may be motivated by malice. Steps can be taken to minimize the risks but if one avenue is closed another may well have been left inadvertently open for the determined saboteur.

2.3 Risk management

In order to deal with the threats facing a system, a risk management methodology can be used. James (1974) identifies the four main stages as follows:

1. Risk identification and analysis.
2. Risk elimination and control.
3. Risk assumption or retention.
4. Risk transfer.

This thesis is concerned with stage 1 of the risk management process. Many authors (Martin,1973), (Fisher,1984) provide a checklist of specific threats that can be used during the risk identification stage. Whilst these can be useful, they are of limited value when identifying risks in ATM, EFTPOS, credit card, Home banking, and wire transfer services. Since electronic banking applications are very different from the usual data processing operations, such checklists are not able to pinpoint the many, very specific, weaknesses of electronic banking services. A more structured approach to risk identification is required.

For every component of the computer system, hardware, software, data, communications and the environment, it is necessary to know what damage, if any, can be caused by each of the major threats : disaster, accident, error, computer abuse and sabotage. A model, therefore, has been set up that allows this to be done. In the following matrix (See figure 2.2) the column headings are the elements of the computer system in need of protection and the row headings are the threat categories. At any intersection in the model, questions can be framed about how a specific asset can be affected by a particular risk e.g. how can hardware be put at risk by disaster? This model has the following advantages:

1. It provides a starting point for a detailed analysis of risks.
2. By working through the model systematically all the major risks may be identified
3. The framework provided by the model allows a clear, easy to follow, description of the risks in electronic banking services .

	Hardware	Software	Data	Communications	Environment
Disaster	X	X	X	X	X
Error	X	X	X	X	X
Accident	X	X	X	X	X
Computer Abuse	X	X	X	X	X
Sabotage	X	X	X	X	X

Figure 2.2 Risk identification model

Chapter 3
The Use of Computers in Banking

3.1 Introduction

In what might be termed the information age, banks have invested heavily in technology to provide the customer with the many services they offer. As with most new technologies, there are problems with its introduction, particularly in view of the banks' dependence on data. The security implications of this are dealt with later. First, though, it is necessary to review the use of computer systems by financial institutions. The hardware, the nature of the data stored, the problems inherent in setting up a network, its configuration and the requirement to protect messages through encryption and message authentication codes, and the many types of software that have to be available are all reviewed. Some features that are specifically associated with the electronic transfer of funds, the use of cards and Personal Identification Numbers are also examined. This application independent information provides the foundation for the discussion in later chapters of the applications and the identification of risks, and is intended to avoid the tedious repetition of detail.

3.2 Hardware

Because of the volume of operations a bank will normally have a mainframe installed. This is made up of a central processing unit, main memory, operator console(s) and auxiliary units for input, output and storage. The reliability of this equipment is a problem for a bank since hardware failure may cause processing to halt. These components have varying degrees of reliability. Data on the mean time between failure (MTBF) and mean time to repair (MTTR) is available from manufacturers. An organisation has to take both this information and the criticality of a piece of equipment into account when deciding which components to duplicate (the central processing unit is very reliable but its failure shuts down the system). Moreover, a computer is highly dependent on its power supply and if this is cut processing is halted. The only way a

bank can be secure is when all the important elements including the power supply are duplexed. Many banks have installed a transaction processing system such as a Tandem Computer NonStop TXP that offers fault-tolerant operations and modular expansion to allow for incremental growth. Such a system can be configured with several processors so that no single fault can cause a halt in processing (New Zealand Computer Scene, 1987). Unfortunately, not all financial institutions are so sophisticated; all that can be assumed when identifying risks is that a mainframe is available for processing transactions. The mainframe is generally linked to a front-end processor which, for the purposes of this thesis, is treated as part of the communications network (see section 3.4).

3.3 Data

Data exists in many forms in electronic banking systems and serves many functions. It can be classified in the following way :

1. Identification Details

   All electronic banking services require the identification of the customer, traditionally the signature on a cheque. In ATM, EFTPOS and credit card services, the customer carries a card that contains information such as the customer account, customer name, and other more specific information that is required by the organisation. The possession of a card alone, however, is insufficient to identify a user to the system; lost or stolen cards are very common. Some authentication process is required and many banks require customers to enter a code or password, a personal identification number (PIN), which is known only to themselves. This effectively acts as a customer signature. Similarly, in home banking and wire transfer services, the user has to prove in some way (user identification, password) that he is the person authorised to initiate the transfer of funds. Wire transfer systems also expect the operator to provides a user identification and password.

2. Customer information

The customer name, address, account number and relevant details, date, type of transaction, amount and account balance, are kept on the master files that make up the database. Some other application-dependent information may also be stored. For example in home banking the account numbers to which money could be transferred may also be stored. The master files are updated as necessary by the data generated by transactions. In on-line systems, to ensure that none of these details is altered during transmission, a message authenticating code (MAC) is usually appended.

3. Financial Information

In order to balance their accounts, banks have to total the credits and debits to customer accounts. Information also has to be kept regarding monies due from or owing to other banks. Other files such as the suspense account which contains unreconciled items are normally maintained.

4. Audit and control logs

A great deal of information is kept as a check to make sure that the system is working as it should. An audit trail is usually maintained to ensure that all the data is processed; the correct data is processed; the data is processed accurately and in a timely fashion; and that mistakes made are corrected (Royal,1987). Fundamental controls such as hash totals and transaction counts are usually in place so that any attempt to alter account information can be detected and logs of all the transactions maintained. Files of passwords and tables of access rights are also kept.

3.4 Communications

An on-line system depends on communications to connect terminals to the computer. The key components of a network are shown in figure 3.1. Since networks are of crucial importance in electronic banking applications, the function of each component is briefly described.

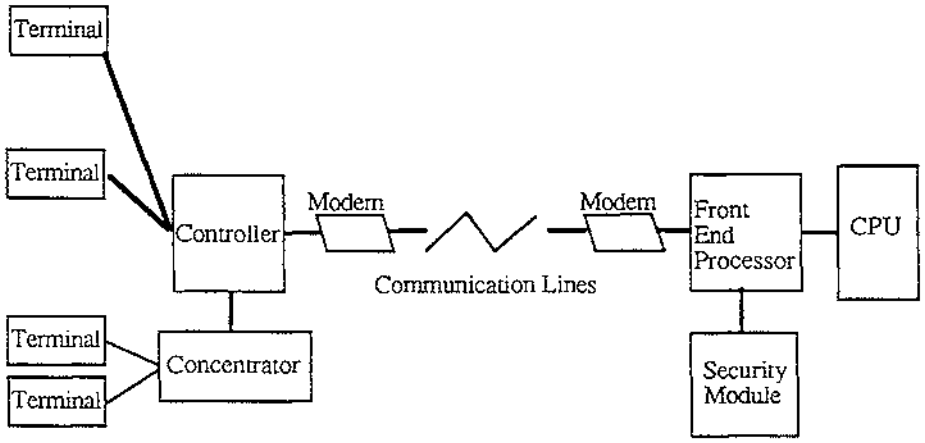


Figure 3.1 Network components

1. Modulator/Demodulator (Modem)

   This is used at one end of the communication line to change the digital signal from computers and terminals into analog signals for transmission over telephone lines, and, at the receiving end, to convert the information back into digital form. Newer digital services do not require this.

2. Controller

   A controller is responsible for the management and operation of a cluster of terminals and may provide for off-line operation when the main computer is not available. The controller may be able to capture and record transactions.

3. Communication Lines

Transactions are transmitted across communication lines usually provided by a common carrier . These telephone lines may be analog or digital. As mentioned above, modems have to be used in conjunction with analog lines. The transmission media can be wire cable, microwave, satellite, optical fibre or possibly a combination. The services offered by the common carrier generally include switched connection (often referred to as dial-up lines), leased lines and packet switching. With a switched connection , the communication line uses any voice transmission wire available. Leased lines, in contrast, are of a better quality with the telephone company guaranteeing the path used. Packet switching facilities transmit messages through a network to their final destination in fixed-length packets and are route independent..

4. Security and Line Monitoring Devices

These are used to encrypt data as well as checking the transmission quality of the line. All aspects of the network can be monitored and a central operator is informed of problems or failures.

5. Transmission Recording Devices

Transactions to be transmitted may be recorded on a variety of media, hard disk, floppy disk or tapes, at both a send point and receive point in a network. This provides a backup facility that can be used if it is necessary to recover after a crash.

6. Concentrators and Multiplexers

Concentrators and multiplexers are line sharing devices that allow many terminals to access a common circuit. The main differences between the two devices are as follows (Stamper,1986) :

- a concentrator is a computer that can perform data processing functions such as polling
- a concentrator is used by itself (at the remote end of the circuit) whilst multiplexers have to be paired
- a concentrator can have a differing number of incoming and outgoing lines whilst a multiplexer takes a certain number of lines onto one line and converts back to the same number of lines.

7. Front-end Processors

A front-end processor takes over the line and terminal management work from the host computer and so is sometimes referred to as a communications controller.

To allow all the components of a network to communicate with each other, standards (national or international) for interfaces and protocols are used. (Protocols are rules which allow entities to exchange information in an orderly and secure manner). The Reference Model of Open Systems Interconnection defined in CCITT, X.200 describes a 7-layer model for communication systems. Levels 1 to 5 are concerned with the communications sub-system whilst levels 6 and 7 are concerned with the application interface. IBM introduced its own standard for networks in 1974, System Network Architecture (SNA). This is widely used in banking as much of the hardware has been purchased from IBM.

3.4.1 Network design

The economics of electronic banking have meant that networks shared by organisations are superceding proprietary systems. The advantage of local competitive advantage cannot justify the required investment in hardware and communications. There are various ways that a shared network can be configured; they all require the setting up of a

"switch" , that is a computer running a piece of software able to deal with the interchange of information (Orkand Corporation, 1983) :

1. Single processor sharing

   With single processor sharing, the complete account files or customer balances of one or more institutions reside at a central facility. The terminals of the member organisation are on-line to a single computer which is used as an authorisation database (see figure 3.2). Transactions are captured by the processor and, when necessary, information is relayed to the host at a later time.

2. Front-end switch

   One central facility is provided for the routing of messages to individual institutions. All the terminals are connected to this computer. It is because messages are sent to the switch before transmission to a data processing centre that the term front-end applies (see figure 3.2). The volume of traffic and the susceptibility of the system to failure with its reliance on one node are the major problems with this approach.

3. Back-end switch

   A terminal is linked in the first instance to its owner's host computer. If the transaction is for that institution then it is processed otherwise it is transmitted to the appropriate institution by the switch that is behind the data processing centre (see figure 3.4). Each institution maintains controls of its terminals but a large proportion of transactions may need to be switched to other institutions. This requires a considerable commitment to backup and recovery as well as the need to decrypt and re-encrypt transactions before further routing.

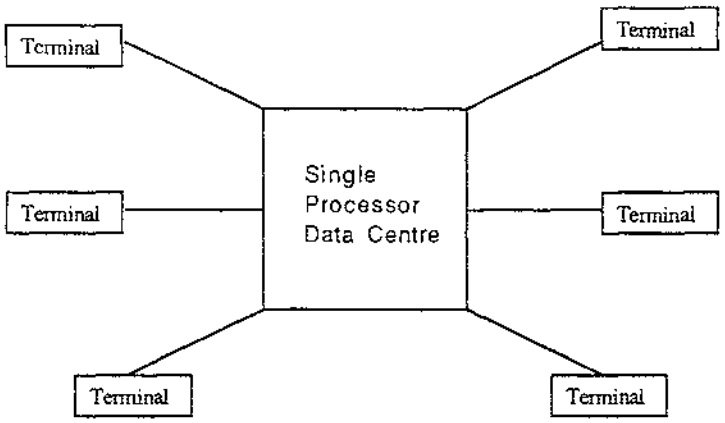


Figure 3.2 Single Processor Sharing (Orkand Corporation,1983)

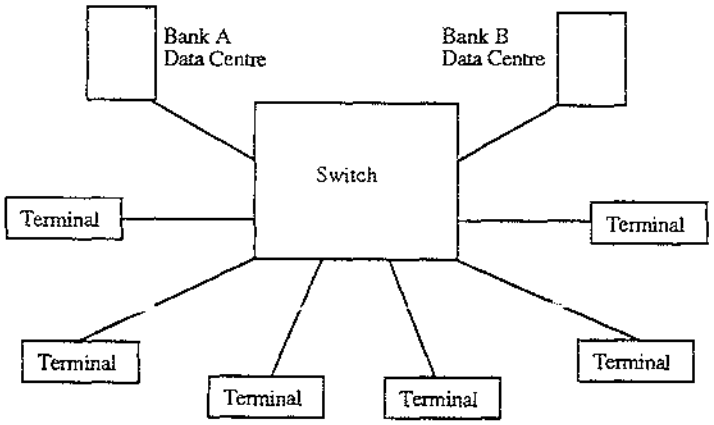


Figure 3.3. Front-end Switch (Orkand Corporation,1983)

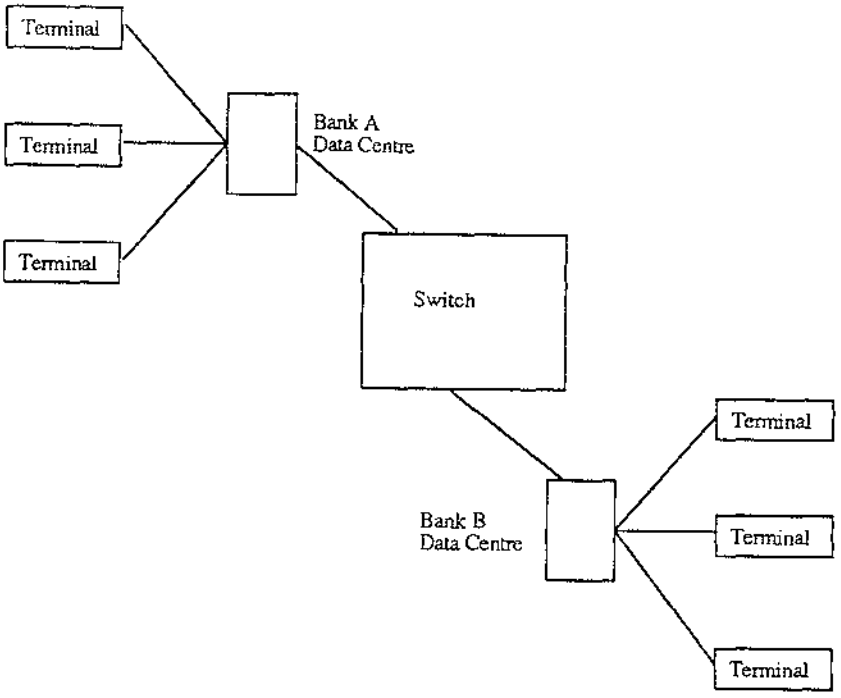


Figure 3.4. Back-end Switch (Orkand Corporation,1983)

4. Local area controller approach

This is a variation on the front-end switch approach and allows for several sites, not only one, to route messages to participating institutions (see figure3.5). Local area controllers are distributed throughout the network as transaction volumes dictate.

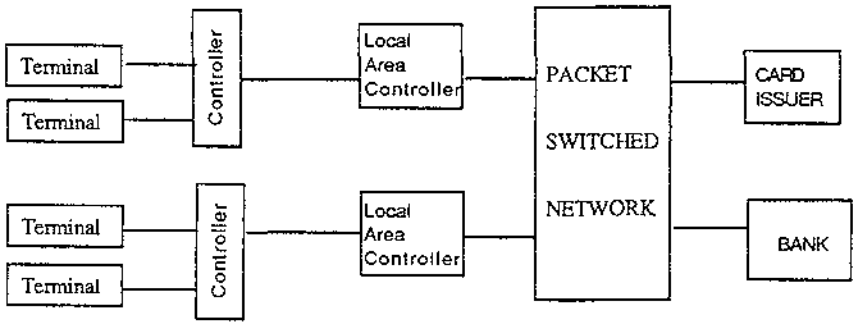


Figure 3.5 Local area controller

5. Hybrid approach

This configuration is a combination of front-end and back-end switches. It allows for a flexible interconnection of institutions at the cost of greater complexity.

3.4.2 Message types

Many messages flow through on-line systems; they can be categorised as follows (Databank,1986) :

1. Authorisation messages

An authorisation request seeks approval for a transaction to proceed whilst the response carries the answer. It should be noted that this message does not carry sufficient information to allow the transaction to be processed.

2. Financial transaction messages

A financial transaction request asks for transaction authorisation but differs from the previous message in that approval results in the immediate application of the transaction. Again, the response contains the reply to the original message.

Further instructions, transaction advice and transaction advice response, can be used by banks to keep each other informed of completed transactions.

3. Reconciliation messages

Reconciliation messages relate to the balance information held for interbank settlement and allow for the settlement of accounts between the participants.

4. Reversal messages

A reversal message originates with the institution acquiring the transaction; it states that the authorised transaction cannot be processed (a reversal is usually the result of a system or communication problem). In contrast, a reversal message (ISO) informs the institution that the instructions transmitted cannot be carried out.

5. Network interchange messages

Network management messages allow the interchange of information about the condition or security of the system.

6. Administrative messages

Administrative messages allow the participants to exchange information on organisational issues.

7. File update messages

File update messages ask that a transaction can be applied to the database. The reply indicates whether action was taken or not.

3.4.3 Encryption

Problems inherent in on-line systems include the transmission of incorrect data and the risk that messages will be disclosed, altered or substituted during transmission. Error checking procedures such as parity checking or block sum can usually detect corrupted

data that requires re-transmission of the message. Errors are not inevitably detected since if two bits are changed accidentally the parity bit will still appear correct to the receiver. If someone is intentionally trying to interfere with the transmission of messages, error detection codes offer very little protection.

Two further safeguards are commonly used, encryption and message authentication codes. A message or a component of a message, such as a personal identification number, can be encrypted to make it unintelligible to anyone who does not possess the decryption key. Encryption is used not only for encipherment but also in the generation of an authentication code. A message authentication code (MAC) can be appended to the data so that any change to an item of information will be discovered. Encryption and MAC processing are examined in more detail below.

Encryption is a process that allows information to be scrambled in some way so that an opponent cannot retrieve the original text. Both code and cipher systems can be used for this purpose but, in computing, cipher systems have been developed as they allow for a change of key. A message, referred to as the plain-text, is encrypted by a key in accordance with specific rules (the algorithm). In this way ciphertext or cryptograms are produced. A key is used so that a large class of ciphers can be defined. The plain text can be recovered by the process of decryption. The basic principles are explained by Davies and Price (1984). Where x is the plain-text, y is the cipher-text, k is the key, E the encryption function and D the decryption function then the result of encipherment is expressed mathematically as

$$y = Ek(x)$$

with decipherment

$$x = Dk(y).$$

It can be seen that the key is a vital feature of the process; it has to be known by both parties concerned but kept secret from others. In classical cryptography the same key is used for encryption and decryption but this is not the case with public key ciphers.

There are various types of ciphers but those used most in computing are block and stream ciphers. With a block cipher the data is encrypted and decrypted in blocks of a size specified by the algorithm. The Data Encryption Standard (DES) and public key encryption which will be described in more detail below can be used as block ciphers. Stream ciphers on the other hand are divided into lengths determined by the user. Chaining is a technique used to make an algorithm more secure since it makes the output block dependent not only on the current data and the key but on previous data in the message. This has the result that even two identical blocks will not produce the same output so there are no repetitive patterns to aid an opponent (a term used in this context to describe a person trying to break a cryptogram). At the start of a message, the previous cipher block is not available so some other information has to be made available for the encryption of the first block. This is referred to as the initialising variable and must be the same for the sender and receiver. To keep this secret, the initialising variable needs to be transmitted in an encrypted form so that it cannot be discovered by criminals otherwise the whole of the first block is vulnerable.

Encryption can be implemented between one node and the next (line-level encryption) or between the devices at each end of the network (end-to-end encryption). With line-level encryption, the message is encrypted for transmission along communication lines only, and is in the clear at a node. Keys only need to be known by the nodes connected by the line. Traffic flow security is provided in this way since all information headers and control signals are encrypted as well as the message. This means that wire tappers cannot even find out where the information is flowing. Unfortunately, the message is held in clear text at each intermediate node.

With end-to-end encipherment the data that is passed through the network to and from the bank has to be encrypted leaving the network information in the clear. The network functions are completely unprotected; "call request" and "call accepted" packets can be detected, so that no traffic-flow security is provided. There is a need for the key to be

available at both ends of the network. There must be a secure channel, therefore, between the two parties concerned for the exchange of the key (this requires good key management techniques, a topic that is considered more fully in chapter 8).

3.4.3.1 Data Encryption Standard (DES)

The Data Encryption Standard (DES) outlines the Data Encryption Algorithm (DEA) announced by the American National Bureau of Standards (NBS) on January 15, 1977 for the protection of non-classified data. The quest for a standard started in 1973 and it became obvious that Lucifer, devised by IBM for use in automated tellers, was the best algorithm available. The original key length of 128 bits was objected to by the National Security Agency on the grounds that its members wanted a cipher "weak enough for them to read but strong enough to protect the traffic against the casual observer" (Athanasiou,1985, p110). After lengthy discussions the DES was agreed upon. Whilst the algorithm was essentially the same as Lucifer, the key length was reduced to 56 bits (plus 8 parity bits).

Classified as a complex recirculating product-cipher, the algorithm encrypts a 64 bit block of plaintext to produce the same length cipher text. Following an initial permutation of the 64 bits, the processes of re-arrangement and substitution of bits takes place 16 times before a final permutation produces the output. The message is recovered by applying the algorithm to the cipher text. The DES can be used as either a block or stream cipher. In Electronic Code Book mode, DES is a block cipher where each block of the message is encrypted independently of the others. Cipher Block chaining, used in the generation of MACs, makes the cipher text dependent on the contents of the previous block (or initialising variables in the case of the first block) whereas in Cipher Feedback mode, the DES acts as a self synchronising stream cipher. Whilst the DES can be (and is) implemented in either hardware or software, only hardware implementations of the algorithm tested and validated by NBS comply with the standard. In practice, large scale integrated (LSI) chips are used for this purpose in banking.

It is impossible to leave this topic without mentioning the DES debate that has raged during the last ten years. From the time that the DES was adopted there were many people who believed that the key length of 56 bits was too short. Hellman and Diffie suggested in 1977 that it would be possible to build a computer that could test a million keys per second(Athanasiou,1985). This machine, it was claimed would break an encrypted message in about half a day for an average cost of US$5000 per solution. Nonetheless many experts considered that the DES was a safe and efficient algorithm for commercial use and the DES was re-certified by the National Security Agency (NSA) in 1983 (Anderson,1987). The NSA have finally decided, however, that current technologies such as supercomputers and fifth-generation software threaten the security of DES and it should be replaced by codes distributed and regulated by NSA (Anderson,1987).

3.4.3.2 Message Authentication Code (MAC)

A valid message authentication code proves that the message is genuine; that is the details have not been changed. The ANSI X9.9 FIMAS Standard recommends a method of authenticating a message that has been widely followed. Using as input the bits of the message that require protection, the MAC processing algorithm produces a new value that is appended to the message. The Data Encryption Standard (DES) is used in conjunction with the relevant bits of the message to produce the MAC. Since DES only operates on 8-byte blocks, in this example, the message is divided into three 8-byte blocks. Block 1 is encrypted by DES and the output is the 8-byte block marked as TEMP1. The result is exclusive ORed against message block 2. This allows the bitwise combination of block 2 with TEMP 1. The result of the exclusive OR is input into DES again, generating TEMP 2. Finally TEMP 2 is exclusive ORed against block 3 with the result input to a final pass through DES (see figure 3.6)

The 8 byte block generated is referred to as the residue. The 32 most significant (or left-most) bits of the computation, called the MAC, are added to the end of the message prior to transmission. On receipt of a message, the host computer calculates a MAC from the data. If the transmitted value is not the same as that computed then the message will not be accepted when the communication protocols indicate an error free reception. The hardware or software must indicate to the computer or operator that a message has failed the MAC test. It has been estimated that the probability of detecting a change in the message is 0.999999998 since a feature of the MAC algorithm is that if any bit of the message is altered then the output of the computation will change. The use of an encryption key known only to the sender and receiver means that it is impossible for someone who knows the MAC algorithm or has captured and analysed messages to duplicate a MAC.

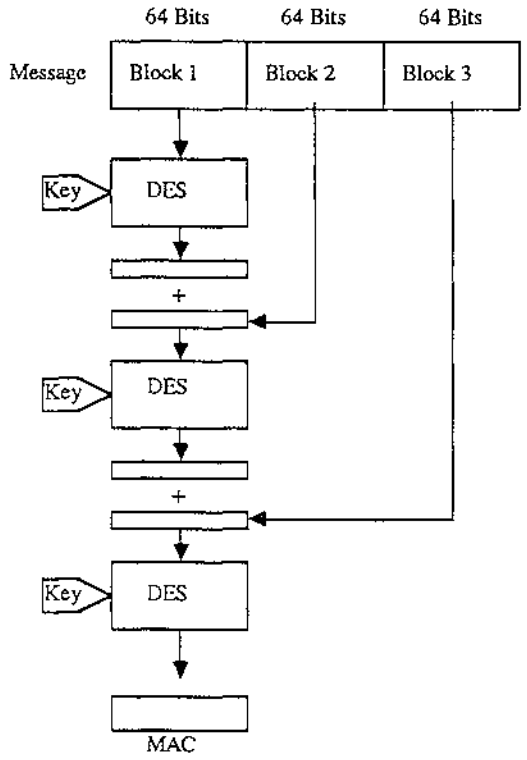


Figure 3.6 MAC Processing (ANSI X9.9,1982)

3.4.3.3 Public key ciphers

The invention of two key cryptography has been attributed by Kahn (1983) to the NSA as well as to the authors of first published paper on this topic, Diffie and Hellman (1976). In this type of system the sender and the receiver use different but related keys only one of which needs to be kept hidden. The sender encrypts a message with a key that is made publicly available (hence the name of the method) whilst the receiver uses a key that has been kept secret to decode the information. This asymmetric system makes it unnecessary to carry a secret key between two locations in order to set up a key. Public key systems are effective because it is extremely difficult to determine the inverse of the enciphering function. The most well-known public key encryption method is that devised by Rivest, Shamir and Adleman (1978) of MIT which can be used to keep messages secret and also authenticate them. The public and private keys are generated using prime numbers and modulo arithmetic. The security of this approach rests on the fact that the product of large prime numbers is very time consuming to factorize even with the use of a computer. This method is slower to use than the DES since the key is so large that the number of computations required is greater.

3.5 Software

The software required to support electronic banking can be classified as : system, security, applications, database and communications. Some of these programs will be purchased from manufacturers or software suppliers whilst others may be written by the organisation itself. The types of software are briefly described below.

1. System software

   This refers to the operating system and utility software (compilers, editors etcetera). The role of the operating system is particularly important as it is responsible for allocating resources to application software, performing input and output operations and maintaining user, program and file access controls. Utility

commands can be very powerful and allow the copying or dumping of data and software.

2. Security software

Software security systems such as IBM's Resource Access Control Facility (RACF) provide various controls for the identification of users and the specification of their access rights to data and programs. Usually logs are kept of authorised and unauthorised attempts to access the system so that continuous monitoring takes place.

3. Database Management Systems (DBMS)

The database software manages the stored data, that is the master files of customer information accessed during programming. Some authorisation controls over the access to data can be performed by the DBMS. It is also responsible for the recovery of the database after a failure such as the following (Orkand,1983) :

- loss of, or problems with connection to a terminal
- loss of, or problems with the network
- loss of, or problems with the connection to a card issuer computer
- loss of, or problems with the connection to a bank or financial institution computer.

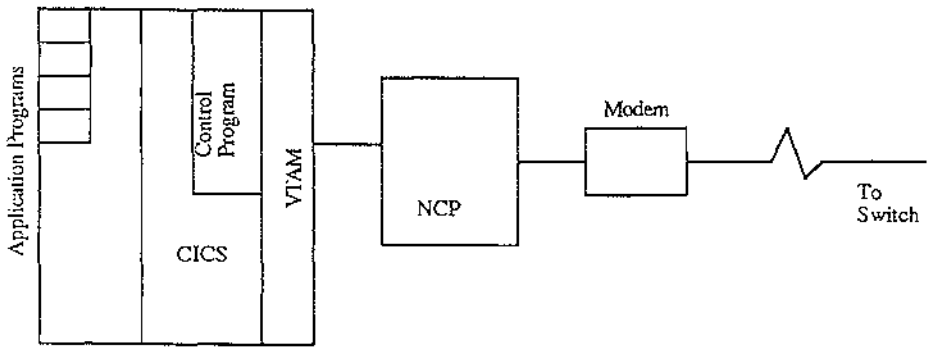
4. Application software

Application programs specific to each electronic banking system have to be written. These include not only the code to update the master files but also programs to generate reports, produce the required balances and compute any totals required for auditing purposes. These programs might be written by the organisation concerned or bought from a software company.

5. Communication software

The controller's software interfaces between the host's access method and the lines to attached devices. It carries out some or all of the following functions depending upon the network configuration : polling and selecting, automatic dial-up and answering, code conversion, message switching, transaction logging, error detection and correction. The access method allows an application to be connected to its associated terminals. Since a fast response time is essential in on-line processing, a teleprocessing monitor like CICS (Customer Information Control System) with its associated message processing programs can be used to take control. CICS is able to act in some respects like the operating system (it starts and stops tasks, manages the memory in its partition and implements a priority system) so that it can quickly connect database records with the appropriate application.

For certain applications, network control software has to control the link with a switch, initialise the line for each session, maintain the encryption keys, generate and verify message authentication codes, control the security module and passes transactions on to the required processing software. Figure 3.7 shows the application programs, CICS and VTAM (virtual terminal access method) in main memory on the host computer with the NCP (network control program) resident on the controller, in charge of the link to the switch.



3.7 Communications Software (Ritchie,1987)

6. Software at the switch and other nodes

The various functions of the switch software include message routing and the driving of terminals (Orkand,1983). It may also be necessary in applications where banks share a network for the software to collect the information needed for inter-bank settlement.

7. Software at a terminal

The resident software carries out functions appropriate to the application in question. Software may be responsible for the capture of the transaction, the checking of a PIN in off-line systems, the encryption of a message, the generation of a message authentication code, dispatching transactions, receiving and checking the authenticity of messages from the host, acting upon the instructions dispatched and the printing of a receipt.

3.6 Cards

The financial institution has the responsibility for issuing cards, setting up any required authentication procedure, processing transactions and sending out monthly statements. Lists of lost or stolen cards, expired cards and cards withdrawn for over-spending must also be produced. Cards are usually issued for two or three year periods. This gives the institution the opportunity to review the history of customers and withdraw the cards of unsatisfactory customers. Finally, and most important, a decision has to be taken about the technology used in the cards.

Card-issuers generally rely on outside firms to manufacture, emboss and distribute cards to customers. From a master file of account information the card production instructions can be generated. The cards are then mailed to the customers after being placed in envelopes by members of staff or by an automated process. If the PIN is selected by the bank it may be sent in a separate posting or collected from the bank. Two types of card

are currently in use : the magnetic stripe and the smart card although it is likely in time that the smart card will replace the magnetic stripe.

3.6.1 Magnetic stripe technology

Currently a user is generally identified to the bank's system by a plastic card and PIN. The customer name, account number and expiry date are embossed on the card and may also be stored on the magnetic stripe. To reduce the possibility of fraudulent reproduction of magnetic stripe cards, secure properties such as a hologram, radioactive or magnetic interleaved bar can be added. These features are illustrated in figure 3.8 .

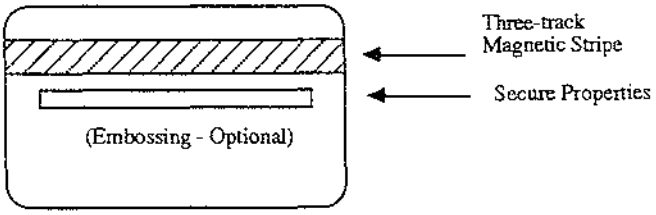


Figure 3.8 Magnetic stripe card (Lipis,1985)

The reverse side of a card contains a magnetic stripe with three tracks. In the United States of America the three track configuration is specified as follows (Bank Administration Institute, 1983) :

Track 1:

This is known as the IATA (International Air Travel Association) track. It provides for 79 alphanumeric characters and is used in a read only mode. Track 1 contains the customer name and account number and is not used in banking applications.

Track 2:

This is specified by the American Bankers Association. It can contain up to 40 numeric characters. The account number, expiry date of the card and optional data is stored here. The information on this track is intended for use in on-line systems and is read only.

Track 3:

This is reserved for the retail banking systems. It allows up to 107 numeric characters to be stored. Since this track can be both read from and written to, it is used for off-line operations. The primary account number (PAN), account number identifiers, offset number and information about the algorithm used to check the PIN are generally kept here. User data that can be updated in off-line mode is also held on this track including the number of withdrawals made in a day or the amount of money remaining that can be withdrawn in a 24 hour period.

3.6.2 Smart card

Since 1986 there has been world wide interest in the potentialities of the smart card for use in EFTPOS, credit card and home banking systems. France was the leader in smart card technology with the practical work being carried out by Roland Moreno in the 1970s. It seemed initially that only the French would use smart cards but now they have been followed by Norway and Luxembourg in Europe whilst the United States of America and Japan have started to show interest (Tutt,1987). It has been predicted that in both of these countries there will be 100 million cards of this type in use by 1990 (Brown and Brown, 1986). A smart card was introduced into New Zealand during 1987 by the Asset card network (Ceramalus,1987).

Smart cards are of the same size, shape and thickness as magnetic stripe cards but differ from the latter by the addition of a microprocessor and memory embedded in the plastic. McIvor (1985) describes the technology used in their making. The nonvolatile, programmable read-only memory allows the storage of information such as the balance of the account and the amount of a transaction. In this way a record of transactions can be built up. The processor controls the interchange between the memory and the various external devices that read the card and enter data (see figure 3.9). The processor architecture is designed to ensure that an area of the card's memory is physically or

logically inaccessible to anyone but the card issuer. The card can be placed in an ATM or card-reading unit connected to a computer.

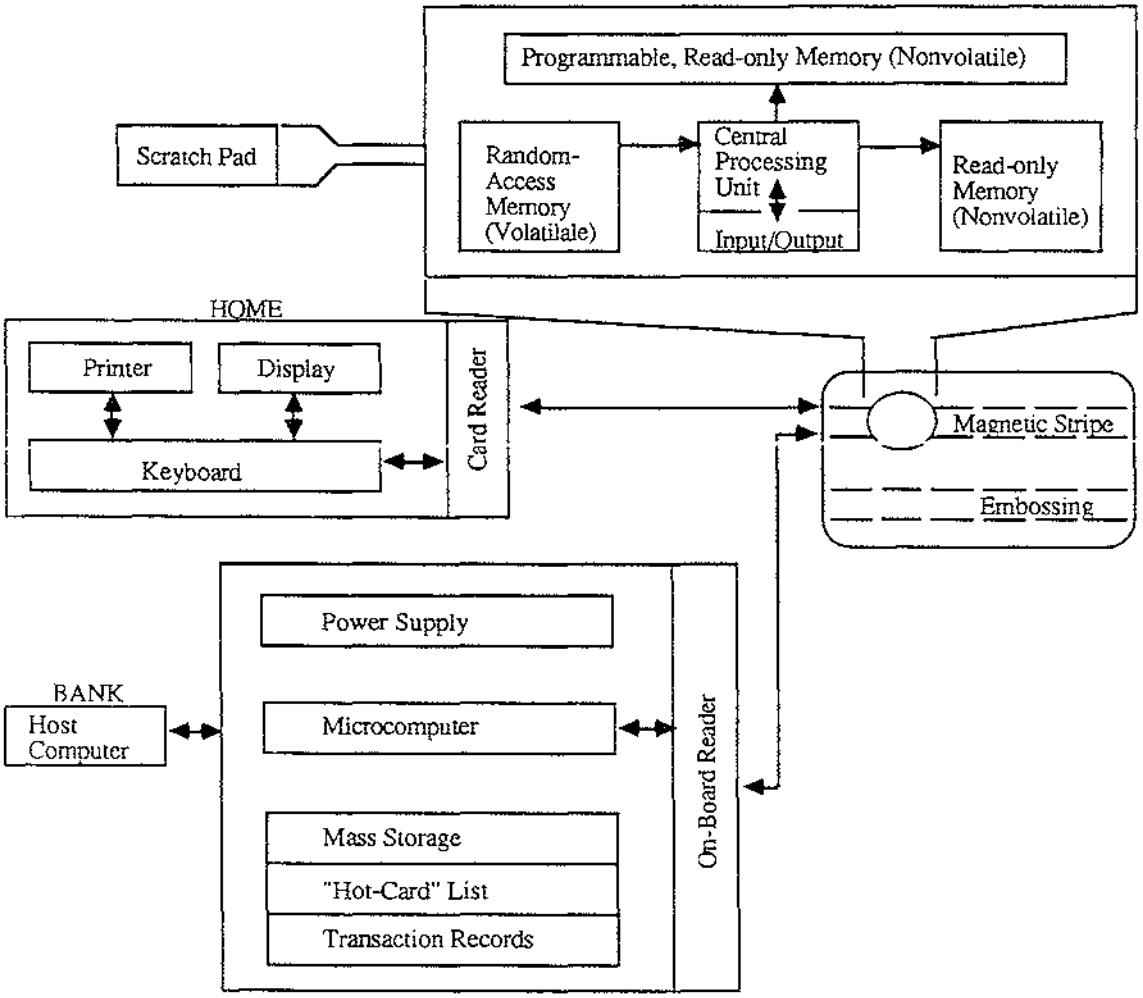


Figure 3.9 Smart card (McIvor, 1985)

A typical smart card is made so that the transparent outer layers protect the chip or chips. The magnetic stripe and signature panel are bonded by heat to the surface of the card. There are eight contacts attached, each one measuring 2mm by 1.7mm and a silicon chip is embedded in a plastic card so that it is flush with the card surface. Contained within these integrated circuits is the microprocessor and the memory. Three types of memory are available on the chip, Read-Only (ROM), Random-Access Memory (RAM) and Programmable Read-Only Memory (PROM). The interface from the chip to the computer is provided by data transfer circuits that operate once power is supplied

1. Read-Only Memory

   Read-Only Memory is non-volatile, that is its contents are not lost once the power supply is removed. The card's operating system and any necessary programs are entered during the manufacture of the card and cannot be subsequently tampered with. The microprocessor executes these programs to monitor use of memory, authenticate users, process transactions, encrypt data, etcetera.

2. Random-Access Memory

   Random-Access Memory is volatile so that any information stored there is lost once the power is disconnected. It is used by the processor as a calculation area to store the intermediate results of arithmetic operations.

3. Programmable Read-Only Memory (PROM)

   Programmable Read-Only Memory which is non-volatile, contains the open, secret and working zones . The information stored in these zones includes the card number, the PIN and the cardholder's name and address. Two types of PROM are available, erasable PROM known as EPROM or electronically erasable PROM referred to as EEPROM. EPROM has the disadvantage that when all the space in the PROM memory has been filled then the card has to be returned to the

manufacturer where, by use of ultra-violet light, the information can be erased. With EEPROM, however, the memory can continually be cleared and updated.

4. The zones in PROM

The need to provide different levels of security for the data kept in memory has led to the provision of three zones in PROM - the open zone, the working zone and the secret zone. Any publicly available information, cardholder name, account number etcetera is held in the open zone whilst transaction details are kept in the working zone. The current credit limit and number of transactions made within a certain time period are also stored in the working zone. Finally, the confidential code of the cardholder, the confidential code of the issuing organisation and any key for encryption are not made accessible to the cardholder at all but are hidden within the secret zone. This enables the microprocessor to examine the PIN stored there and to compare it with that entered by the cardholder. In this way, there is no need to have the PIN either transmitted along communication lines for checking or verified by an algorithm in the terminal. Also, any encryption required can be carried out by the microprocessor.

3.7 Personal Identification Number (PIN)

The personal identification number (PIN) acts as a user password to authenticate the identity of the user (see appendix 1). There are three principle methods of generating PINS which are briefly outlined below.

1. Derived PIN

Here the PIN is generated via a cryptographic algorithm and key from the customer's account number or some other value uniquely associated by the bank with the individual. The bank then issues this to the customer. Verification of the PIN entered by a customer at an ATM takes place by comparing it with the result

produced by making use of the same algorithm to recalculate the PIN from the information on the card.

2. Randomly generated PIN

A random PIN can consist of numbers or letters or both. A random number generator such as electrical noise, a pseudo-random number generator or the Data Encryption Algorithm can generate numeric PINs. By the use of conversion tables these numbers can be changed to alphabetic characters as required. These values have to be stored in the system to permit verification of PINs entered by customers. Again PINs have to be delivered in some way to customers.

3. Customer selected PIN

A customer is permitted to select a group of letters or numbers that, hopefully, constitutes an easily memorised combination. This combination might be stored on the computer for the purpose of subsequent verification as with randomly selected PINs. Alternatively, it can be used to generate, according to a specified algorithm, a related number that is printed on the card. In this latter case, a check can be made that the PIN entered would produce the number on the card. This procedure is essentially the same as that used with derived PINs.

The use of encryption is central to many aspects of PINs. With derived PINs a key is required at the central computer for the generation of PINs and at terminals in off-line systems for PIN authentication. If PINs are stored for the purpose of verification in on-line systems they are usually held in encrypted files at the central site. The security of keys is, therefore, an issue of central importance. Both randomly generated and, in some cases, customer selected PINs have to be stored on the computer system. To prevent personnel from accessing stored PINs, standards specify that these values should be held in an encrypted form. It is left up to the various organisations to decide whether the encryption is reversible or irreversible. With reversible encryption the system has the

inherent capability of decrypting the stored PIN value and retrieving the clear text PIN. Reversible encryption is useful when periodically all PINs are decrypted and re-encrypted using another key. This may be done regularly to prevent an adversary from compromising the current key. Reversible encryption also allows customers to be re-assigned the same PIN in the case where they have forgotten the value. Finally, reversible encryption provides for the decrypt and compare operation when PINs entered at an ATM terminal are verified. If irreversible encryption is used the PIN value received has to be transformed and the result verified by comparing it with the stored PIN value. The clear text PIN value cannot be decrypted, therefore, from the stored value. In the case of derived and possibly self-selected PINs the offset value may be stored on the plastic card.

3.8 Conclusion

Banks have taken advantage of the revolution in information technology to transfer money in various innovative ways. Many different payment methods are now available to customers. The resulting technological complexity is the price that has to be paid by the banks. Whilst it was once sufficient to keep customer account information, cards may now have to be issued and identification data such as PINs stored. Communications have allowed terminals to be connected up to the bank from homes, offices, retailers and airports as well as from inside and outside branches. To keep such networks running, the hardware, software, and communications equipment all need to be reliable. Encryption may also be required to protect some or all of the transmitted data. It is not surprising in view of the complexity of the technology used in electronic banking that disaster, accident, error, computer abuse and sabotage pose such a threat to security. Whilst security threats exist banks need to protect themselves from fraud. However, genuine customers may sustain the loss if the banks seek to off-load all responsibility. It can be very difficult with real-time, high volume applications to track down the source of a problem. It should always be borne in mind that for every technological advance there are usually some compensating disadvantages.

Chapter 4

A Description of the Electronic Banking Applications

4.1 Introduction

In this chapter each of the five electronic banking applications under consideration : ATMs, EFTPOS, credit cards, home banking and wire transfer, is described from a banking perspective. Since there are many ways these applications can be implemented a typical system is specified in each case. Also, the major security threats are listed for each application together with references to later sections which deal more fully with the risk.

4.2 Automated Teller Machines

Automated Teller Machines (ATMs) are unmanned devices which can handle the same routine financial transactions as the traditional bank teller - accepting deposits, dispensing cash, transferring money between accounts, answering balance inquiries etc. They were introduced to make banking services more widely available to customers. For this reason ATMs are located both off premises as well as on, with 24 hour access in many countries. The growth in the number of ATMs in the last few years has been phenomenal, particularly in the United States of America where 1,935 ATMs had been installed by the end of 1973 but the total in place by 1985 was 73,477 (Zimmer, 1986). An issue of current importance is whether an ATM network should be proprietary or shared. In the first case costs are relatively high per customer but security threats are minimized whereas shared networks reduce capital and running costs but multiply the security risks.

4.2.1 Components of an ATM

An ATM has rather unusual characteristics in that it functions as a safe as well as an electromechanical device that can serve the customer. Typically an ATM consists of a storage chest with a combination lock, cash dispensing machinery and receptacles to hold deposits and the money to be dispensed. Separate slots are available for the deposit or withdrawal of money. Transaction details are entered into the system via a card reader, a

function keyboard and a numeric keypad. Both the message display panel and the receipt printer provide the customer with information about a transaction. Finally, an ATM contains the software and/or hardware required for the processing and transmission of data. The safety of these devices is so important that in the United States of America legislation covers the minimum physical security requirements for ATMs.

4.2.2 ATM operation

To operate an ATM a customer typically inserts a plastic card (see section 3.6.1) into the card input/reader which only permits the entry of cards with specific dimensions and thickness. The information held on the magnetic stripe is read as another check on the validity of the card. Following instructions, the customer enters a Personal Identification Number (see section 3.7) on a 10 key numeric or alphabetic keyboard as shown in figure 4.1.

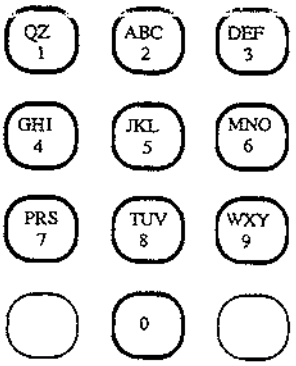


Figure 4.1 ATM keyboard

The PIN, usually four to six characters long, acts as a password to identify the cardholder; this value should only be known to the owner of a card. Usually three attempts in 90 seconds are allowed for a customer to input a valid PIN. If these constraints are not met, the transaction is aborted and the plastic card retained by the machine. After the PIN has been validated, the customer selects the type of transaction desired using the function keyboard. Whilst some devices act only as cash dispensers, others offer a wide variety of functions. These can include :

- withdrawal from a cheque account
- withdrawal from a savings account
- deposit to a cheque account
- deposit to a savings account
- transfer from a cheque account to a savings account
- making a balance inquiry
- cheque book request
- statement request.

The next step depends on the transaction type selected. For withdrawals and deposits the amount of the transaction is entered using the numeric keypad. After this the customer is given the opportunity to change the type of transaction selected and/or the amount before pushing the "Enter", "OK" or equivalent key. For withdrawals a check is made that the balance is sufficient and that the bank's limit is not exceeded. Provided that these conditions are met, cash is issued from the dispenser, otherwise an appropriate message is displayed. When a deposit is made, on the other hand, the customer places an envelope containing the cash in the depository. A receipt is issued in both cases confirming the details of the transaction. If a balance inquiry has been made, the balance is shown in the message display panel or printed on a receipt. Finally, the card is returned to the customer.

4.2.3 Mode of operation

Transactions processed by an ATM have to be reflected in the database of customer records held by the bank. This can be achieved in various ways. ATM services that operate in off-line mode are not connected to the central computer. In this case the ATM may contain all the necessary logic for the processing of transactions and updating the number of withdrawals made but more usually it is linked to a controller (often on branch premises) which performs this task as shown in figure 4.2. A log of transactions produced by the controller is used to update customer files. This file does not have to be hard copy but can be recorded on tape. The file of stolen or lost card numbers (also

known as the negative or "hot" file) can also be kept at this point for checking the validity of cards.

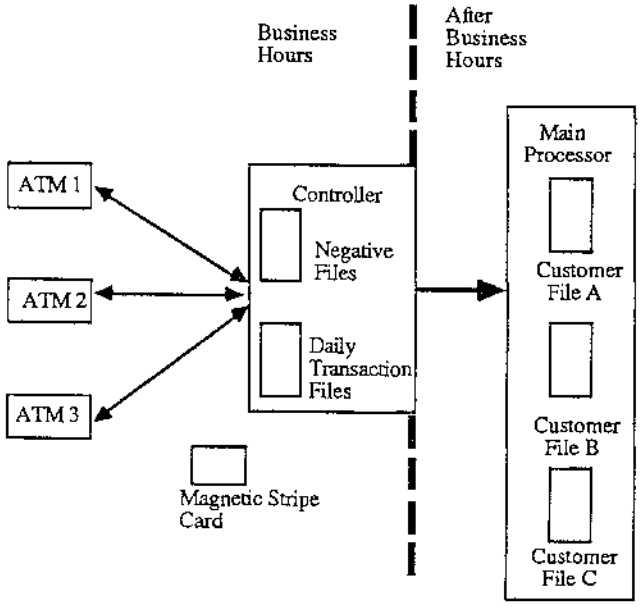


Figure 4.2 Off-line ATM (Orkand Corporation,1983)

An on-line system depends on communications to connect the ATM to the computer. On-line operation, depicted in figure 4.3, allows the ATM equipment to be linked either directly or via telephone communication lines to the bank's central computer. This is a more expensive procedure as communication charges are incurred. It has the advantages though that a transaction is authorised by the central computer and that there is no need to record information on a customer's card. There can be no guarantee that an on-line ATM will not suffer a communications breakdown. Fall back procedures when real-time processing is not available are usually set up so that some services can still be provided. In this case off-line procedures similar to those described above are used temporarily.

A bank may operate an independent proprietary service or join with other banks in a shared service. With a proprietary system, a direct link between the ATM and the computer is set up; there is no need to route messages to the appropriate institution. This configuration is illustrated in figure 4.4. Once banks decide to set up a network there has to be provision for each institution to receive their own customers' transactions.

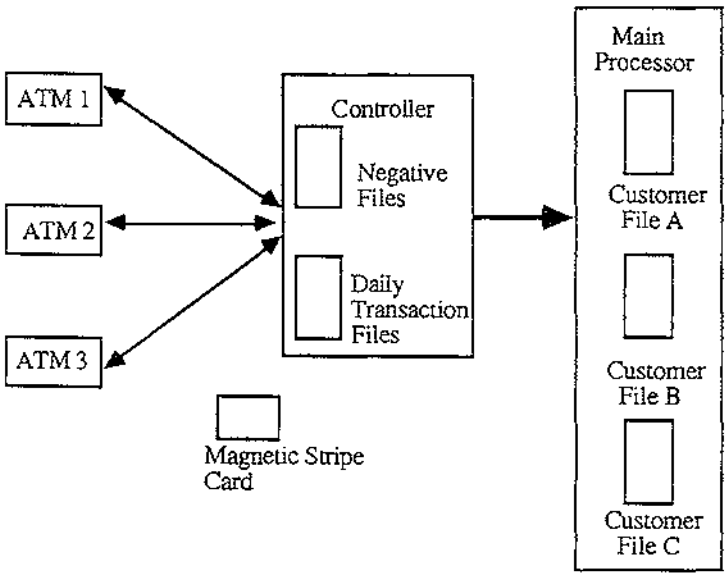


Figure 4.3 On-line ATM (Orkand Corporation,1983)

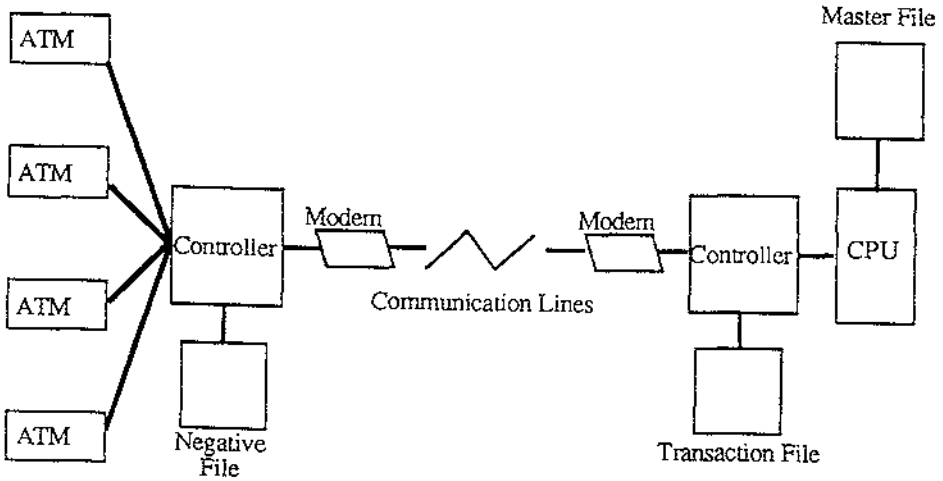


Figure 4.4 ATM network

PIN verification is carried out by the card issuer's computer and not at the ATM since banks use different methods of verification and do not wish to share their secret keys with other institutions. The participating institutions have to decide how messages and PINs can be transmitted securely between banks and make arrangements for settlement at the end of a specified period. The problem of settlement between banks arises in a shared network because a card holder can withdraw cash or make a deposit at any ATM in the network. Consequently, there may be two banks involved in a transaction, the card issuer and the bank operating the ATM. Accounts of these transactions have to be kept by both banks so that settlement can take place at the due time.

There are various ways in which the shared network can be set up, and, as mentioned in section 3.4.1, they all require the setting up of a "switch". With a front-end configuration, transactions are sent to the customer's bank via the switch (figure 4.5). An example of this is the New York Cash Exchange (NYCE). Whilst the participant banks are situated in New York, New Jersey and Connecticut the switch is in Milwaukee. All the banks are connected to this through a multiplexer in Fort Lee.

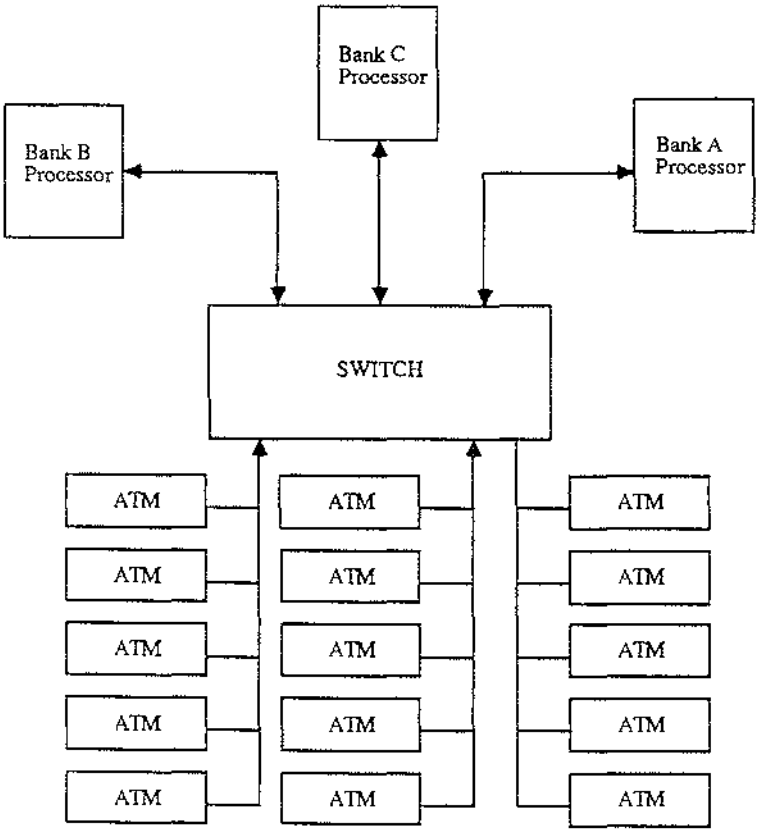


Figure 4.5 Front-end ATM network

When ATM transactions are routed to the computer of one of the participating banks, this is referred to as a back-end switch (figure 4.6). The data centre of the institution has to ask the question "Is this transaction on us?" If the answer is "Yes" then the transaction is processed there otherwise it is directed to the appropriate institution. This is a rudimentary description only of the basic principles involved in ATM networks. In the real world networks are much more complex; hybrid systems involving both front-end and back-end switches often occur.

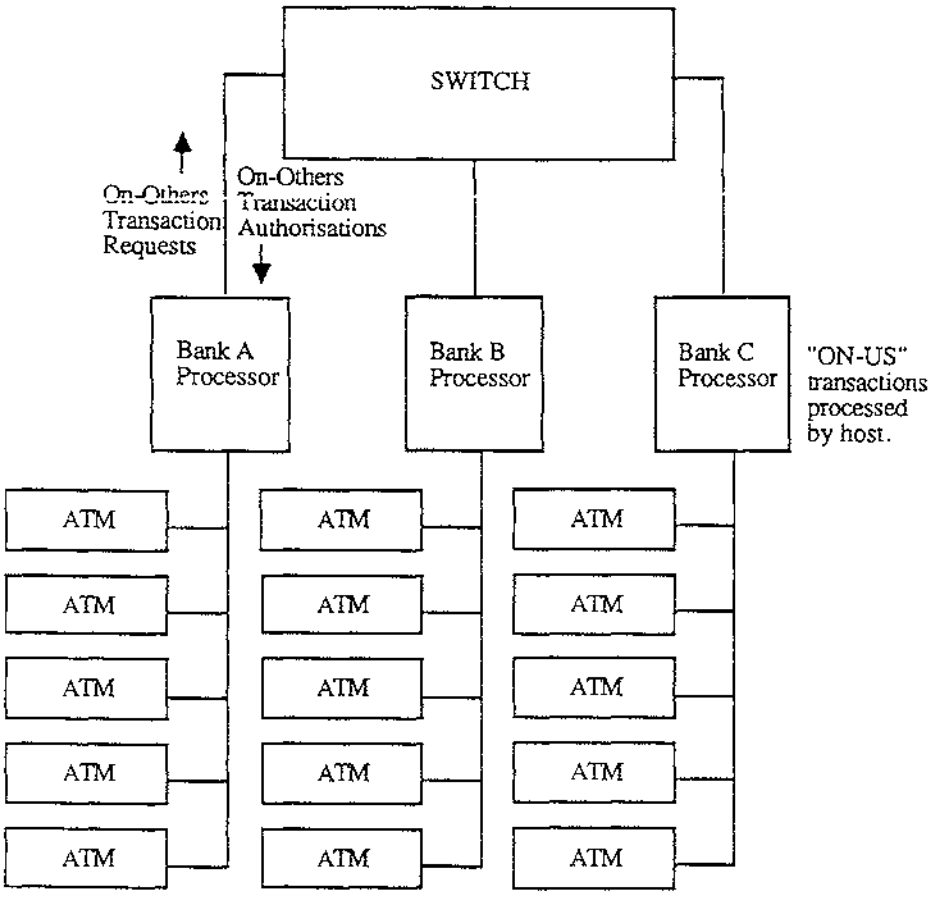


Figure 4.6 Back-end ATM network

4.2.4 Proposed analysis

There is no typical ATM system that can be analysed from the point of view of security. There are differences between off-line and on-line systems due obviously to the fact that the latter uses communications and the former does not. For this reason the risks to both systems are considered. Again, there is a great diversity of on-line systems. The risks to an on-line, shared ATM system which has off-line fall back procedures will be identified. This is justified on the following grounds. Firstly, writers are currently of the opinion that proprietary systems are becoming obsolete, "No one can compete with a shared network." (Shamoon,1986). Secondly, the security problems are more severe in a shared system with its many participants and complex network structure. Finally, permitting both on-line and off-line operation significantly increases the number of threats to the application.

4.2.5 Conclusion

Table 4.1 identifies the major risks that apply to both off-line and on-line ATM applications. Both services for instance would have to stop running if a disaster occurred and no back-up provision had been made. Any ATM is in danger of physical attack from those trying to steal the cash or deposits held there. Sabotage can also be the motive for such an attack. Robbery of customers or employees servicing the ATM also occurs. A terminal can malfunction in a variety of ways : failing to record deposits or withdrawals, paying out the wrong sum or recording an incorrect transaction amount. This may be due to a hardware fault or a software error. The software in the terminal can also be incorrect because of a fraudulent change by an employee. Staff are in a very good position to attack the system. They may steal cash or deposits, make use of captured cards, enter incorrect data, obtain PIN information etcetera, depending upon the opportunities available to them. Since cards and PINs identify customers to the computer system, if they are obtained by others whether bank employees or outsiders, fraudulent transactions can be made.

Off-line ATMs

PIN verification has to be carried out by the terminal in off-line ATM applications. If one key is used by the PIN verification algorithm, the discovery of this threatens all the PINs in the system. Off-line systems have another major problem. Since customer account information cannot be accessed, the balance cannot be checked. Limits are usually put in place on the number of transactions allowed per day and the withdrawal amount. This information is usually stored on the magnetic stripe but can be overwritten using suitable equipment. The customer can then make as many withdrawals as he wants. These risks are shown in table 4.2.

On-line ATMs

Without encryption the PINs transmitted through the network can be discovered. Such an interception can lead to fraudulent cash withdrawals being made. If a message authentication code (MAC) is not appended to the transaction, details such as the amount or account number can be altered. Even when encryption and MAC processing are used, a message may be recorded and replayed through the system. Both requests and authorisation to pay messages can be imitated in this way to withdraw money from an ATM. The use of encryption introduces further problems. Keys are stored in ATMs and criminals may try to force open the area where this is held. If the transmitted PINs are decrypted in main memory for checking, they may be illegally recorded. Moreover, in shared networks, where members have to share at least one key, a breach of security can compromise the network. It is obvious that encryption depends heavily upon the security of the keys in the system. Finally, on-line systems are vulnerable to a hardware or communications failure. At this point, a bank has to decide whether to halt operations or change over to off-line ATM processing. Communications can be disrupted by criminals so that the less secure off-line mode is in operation. Without the real-time checks, large sums of money can be withdrawn. The threats to communications are shown in table 4.3. In addition the risks to off-line systems in table 4.2 also apply when this mode of operation is permitted.

Table 4.1 Principle risks in all ATM systems

(The major risks are identified by the use of bold type face)

Chapter 5

5.2	**Disaster to hardware**
5.3.1	Minor disaster
5.3.2	Malfunctioning equipment
5.4	Error
5.5.1	Interference with hardware
5.5.2	Theft of equipment
5.5.3	Extortion
5.5.4	Misuse of computer resources
5.5.5	Vandalism
5.6	**Sabotage**

Chapter 6

6.2	**Disaster**
6.3	Accident
6.4	Error
6.4.1	**Errors in the software lifecycle**
6.4.2	**Omissions**
6.5.1	**Unauthorised change to software**
6.5.1.1	**Program modification to facilitate fraud**
6.5.1.2	**Program modification to cover up fraud**
6.5.1.3	**Circumvention of security controls**
6.5.1.4	Deliberate error
6.5.2	Methods of attack
6.5.3	Copying software
6.5.4	Extortion
6.5.5	Disclosure of software
6.5.6	**Running unauthorised software**
6.5.7	Rerunning, restarting or cancelling jobs improperly
6.5.8	Opportunities
6.6	**Sabotage**

Chapter 7

7.2	**Disaster**
7.3	Accident
7.4	**Errors**
7.4.1	**Incorrect input**
7.4.1.1	**Erroneous ATM deposit**
7.4.2	**Incorrect processing**
7.4.3	**Incorrect output**
7.4.4	**Loss or corruption of data**
7.4.5	**Omissions**
7.4.5.3	**Phantom transactions**
7.5.1	Unauthorised use of passwords
7.5.2	**Masquerading as a legitimate customer**
7.5.2.1	**Cards**
7.5.2.2	**Discovery of PIN**
7.5.3.1	**Alteration of data input**
7.5.3.2	**Alteration of messages**
7.5.3.3	Error correction
7.5.3.4	**Changing files**
7.5.3.5	**Data alteration during processing**
7.5.3.6	**Additional transactions**
7.5.3.7	**Fictitious deposits**
7.5.4	**Collusion**
7.5.5	**Taking advantage of a genuine error**
7.5.6	Falsification of data
7.5.7	Suppression, alteration or destruction of output
7.5.8	Misuse of output
7.5.9	**Disclosure of data**
7.5.10	**Extortion**
7.5.11	**Denial of valid transaction**
7.5.12	**Theft of data**
7.6	**Sabotage**

Chapter 9

9.2	Disaster
9.3	Accident
9.4	Error
9.4.1	Omissions with regard to ATMs
9.4.2	Unusable card
9.4.3	Failure to protect documents
9.5.1	Unauthorised use of sensitive documents
9.5.2	Theft from an ATM
9.5.3	False claim
9.5.5	Vandalism
9.6	Sabotage
9.7.4	Security
9.7.5	Legal issues
9.7.6	Customer privacy
9.7.8	People

Table 4.2 Additional risks in off-line systems

7.5.2.2	Discovery of key used in the PIN verification algorithm
9.5.4	Crime at off-line ATMs

Table 4.3 Additional risks in on-line ATM systems

Chapter 8

8.2	**Disaster**
8.3	**Accident**
8.3.1	Equipment breakdown or fault
8.3.2	Noise on the line
8.4	Errors
8.4.1	**Failure to provide adequate back-up**
8.4.2	**Insufficient capacity**
8.4.3	Poor quality lines
8.4.4	Omissions
8.5.1	Tapping of communication lines
8.5.1.1	**Passive wire tap attack**
8.5.1.2	**Active line tap**
8.5.2	**Masquerading**
8.5.3	**Between the lines entry**
8.5.4	**Browsing**
8.5.5	**Emulation of equipment**
8.5.6	Disclosure of information
8.5.7	**Extortion**
8.5.8	**Attack on network components**
8.5.9	**Taking advantage of on-going maintenance**
8.6	**Sabotage**
8.7	**Risks to encryption and message authentication**

4.3 EFTPOS

Introduction

Electronic Funds Transfer at the Point of Sale (EFTPOS) is a term that encompasses a wide range of facilities which enable a customer to make payments at a retail location. Lipis (1985) identifies the following services : cheque guarantee, credit and/or debit card authorization and direct debit, that is transfer of funds from the purchaser's bank account to the merchant's bank account. The direct debit when carried out electronically has most interested bankers and retailers. It allows the elimination of paper processing (cheques and credit card transactions), reduces the possibility of fraud by guaranteeing funds to the retailer and speeds up the whole payment process. Consequently this service has become primarily associated with the term EFTPOS and this definition will be used for the purposes of this thesis.

4.3.1 General Principles of EFTPOS

There can be as many as four parties involved in an EFTPOS transaction, the customer, the institution which provides the customer's funds, the retailer and the retailer's bank (the two banks may be the same). As with ATM services, a customer is issued with a card and is expected to know its associated PIN (see section 3.7). Very often the same card can be used in both ATM and EFTPOS applications. The amount of a purchase is entered into the terminal whilst customer details are obtained by swiping the card through the terminal. The transaction is authenticated by the customer entering the PIN into a pad connected to the terminal. An authorisation request is transmitted to the card issuer to check that the customer is the genuine card owner and has sufficient funds available to pay for the purchase. Provided that these conditions are met, the appropriate sum is transferred to the retailer's account. To complete the EFTPOS process a receipt is printed for the customer. The banks have to keep account of the amounts involved so that they can settle up at the end of a specified time period by inter-bank transfer. Lipis (1985) diagrams the process as shown in figure 4.7.

4.3.2 EFTPOS systems

Several EFTPOS systems are available. The principle types of service will be described:

1. Single bank system

   In this basic system, transactions are only processed if both the customer and retailer have an account at the organisation operating the service. After authorisation (if this is given), the funds are electronically transferred from the customer's to the merchant's account.

2. Multiple bank system with off-line transaction processing

   Two or more banks participate in this system which does not allow on-line authorisation of the transaction. The transaction details, the amount of the purchase, the debit to the customer and credit to the merchant, are recorded on magnetic tapes that are sent to a special clearing service which is responsible for settling between banks.

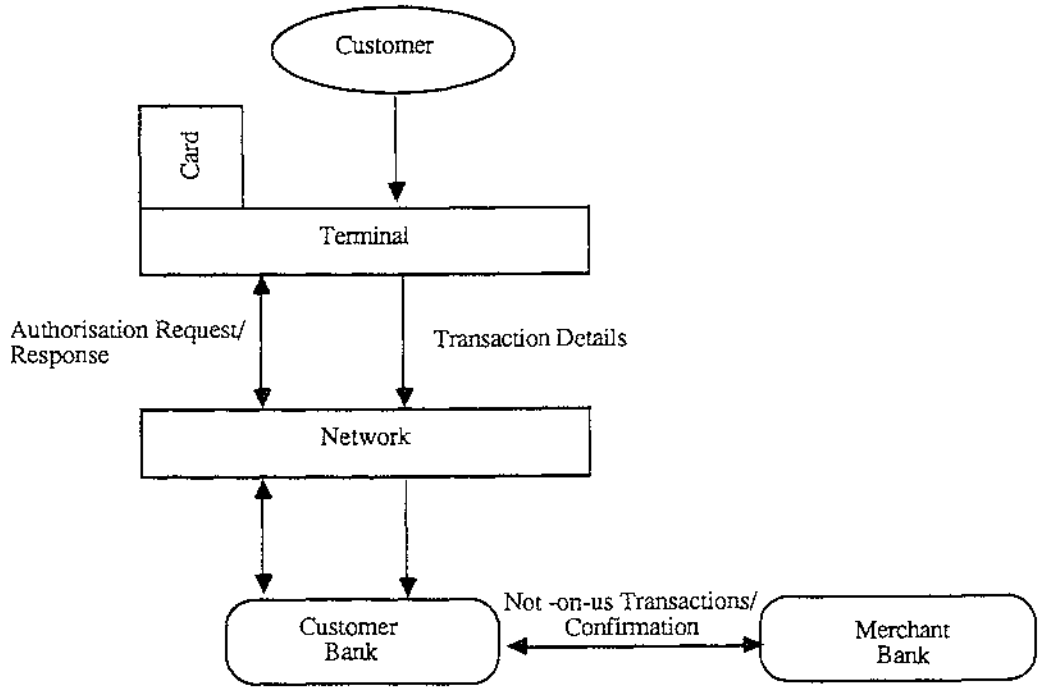


Figure 4.7 EFTPOS system (Lipis,1985)

3. Multiple bank system with on-line transaction processing

Many banks and retailers co-operate in a system that guarantees the transfer of funds, or value as it is often known, to the receiving party. On-line authorisation of transactions is permitted in these shared systems. The retailer's bank is referred to as the acquirer since in many systems it is the processor belonging to the retailer's bank that receives a transaction to forward to the card issuer. Switching centres are used for routing EFTPOS messages in the same way as described for ATM services. If the balance in the account is sufficient and the PIN is verified then the purchase proceeds and the amount is debited. Relevant details are then sent on to the merchant's account to allow the credit to be processed. Davies and Price (1984) describes the natural progression of message as triangular, the request from the terminal to the card issuer, the payment from the card issuer to the card acquirer and the confirmation of payment from the acquirer to the retailer.

There are other types of transaction that the EFTPOS terminal may generate. If the terminal has to be initialised daily by the retailer entering a magnetic stripe card and PIN then this must be authenticated by the computer to which the terminal is attached. Such a procedure is needed to ensure that the terminal is genuine. Another optional transaction is a refund procedure which requires the retailer's card and PIN to authorize it.

Of the three types of EFTPOS systems just described, the last is the one that will be examined in detail since practical considerations dictate that retailers must be able to accept the card of more than one financial institution.

4.3.3 EFTPOS components of a multiple bank system

The major components of such systems are POS terminals, plastic cards, concentrators or terminal controllers, communications network, switching centre and the mainframe.

4.3.3.1 POS Terminal

Terminals in banks or merchant locations are used to input transaction data and to receive the response from the computer or switch. Terminals may be provided either by the bank or merchants. In the latter case electronic cash registers may be modified to provide a POS terminal. Certain features will usually be available (Lipis,1985) :

- a manual keyboard to enter transaction details
- function keys to enter transaction codes and activate preprogrammed terminal functions
- fixed indicator lights to reflect terminal conditions and to indicate standard terminal responses
- a variable digital display for confirming data input and indicating variable system responses
- a terminal memory or buffer which contains a terminal identification code
- a reader which can accept information from a plastic card
- a customer security pad which allows the cardholder to enter a Personal identification number to authenticate the transaction
- a printer to produce hard copy receipts of the transaction.

4.3.3.2 Plastic card

A card using magnetic stripe and/or smart card technology is issued to customers (see section 3.6). There are two principal ways that smart cards can be used in EFTPOS, both on-line and "store and forward" systems can be set up. On-line systems provide for the smart card to be used in conjunction with a terminal linked to a computer, whereas with store and forward systems the interaction is limited to the smart card and the terminal with transaction details passed on to the computer at intervals. The "store and forward" systems are considered only in conjunction with credit cards (see section 4.4.2.1).

On-line systems work in the same way as described in section 4.2.1 except that the customer enters a smart card instead of a magnetic stripe card. This has the advantage that the processor on the smart card can check the customer entered PIN by comparing it with

the code in the secret zone. The transaction details are forwarded to the computer so that a check can be made to see whether the card is stolen and that purchase does not exceed the funds in the account. Finally, if the transaction proceeds, funds have to be transferred from the customer's to the merchant's account. These procedures (Brown and Brown, 1986) are illustrated in figure 4.8.

1) Customer's card is read by the card reader.

2) Transaction details are entered into workstation.

3) Customer enters PIN into PIN pad.

4) Transaction details are sent to card issuer's computer for authorisation.

5) Both the issuer's records and the smart card's memory are updated and a receipt issued.

6) Funds are transferred electronically through the clearing system.

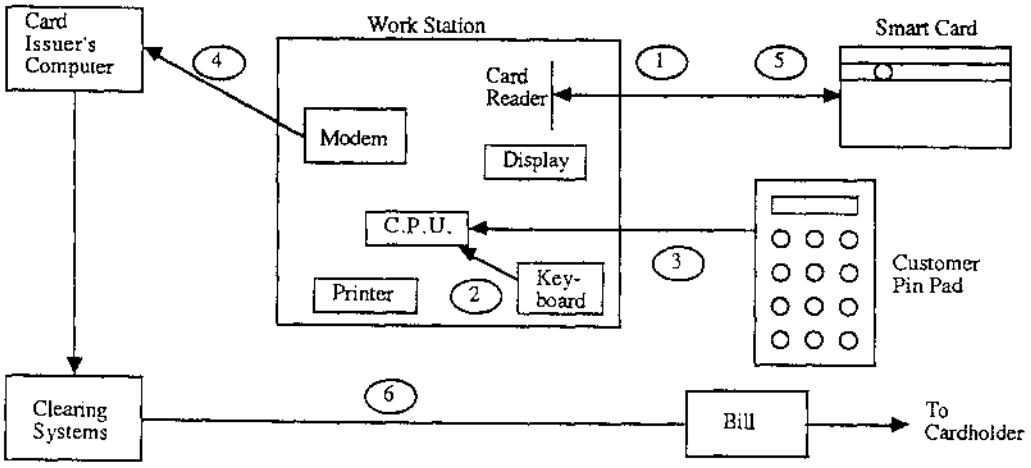


Figure 4.8 On-line EFTPOS with smart card (Brown and Brown,1986)

4.3.3.3 Communications components

The communications network has to be able to connect merchants to the relevant bank system. Groups of terminals can be connected via an in-store controller or a multiplexer to the appropriate network usually by a switch. The function of a switch is described in section 3.4.1. In EFT-POS applications the switch is responsible for routing transaction messages to the customer's bank computing system and switching back the responses. Once a transaction has been approved the switching centre also transmits the relevant funds electronically to the merchant's bank computer system. Whilst the switching centre does not process transactions it does have some processing functions such as the logging of transactions (Lipis,1985).

The various switch configurations have been described in section 3.4.1. With a back-end switch transactions are directed to the cardholder's bank via the computer to which the merchant is connected (see figure 4.9). This has the disadvantage that transactions for other institutions have to be decrypted and re-encrypted for onward transmission. Key management is a matter of great concern; it presents a serious security risk to the network.

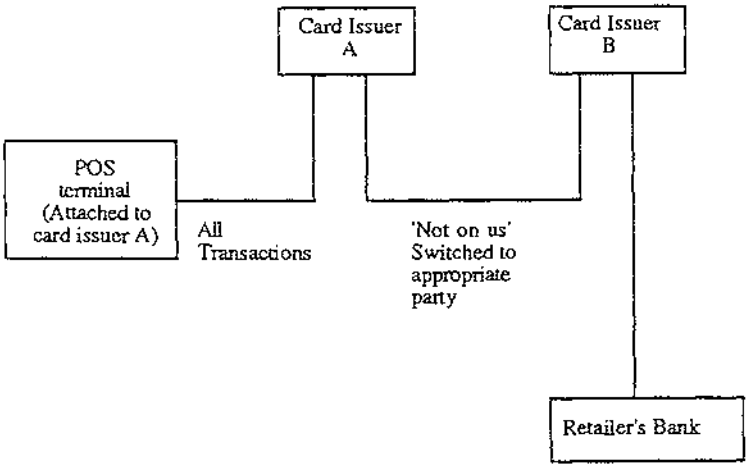


Figure 4.9 Back-end EFTPOS system

Alternatively transactions can be sent straight to the card issuer's bank using a central switch, front-end switch or a transparent transport approach. If a transport transparent network is used then the terminals will be directly connected to the appropriate host computer. The link can be set up either by the telephone network or the packet switching network. The major disadvantage of this system is that every terminal must be able to encrypt data using the algorithm and keys of every card issuing institution. For this reason packet-switching is not generally used by itself (although it may be combined with a front-end or central switching system) and will not be further considered. In open access systems (that is where retailers can accept any EFTPOS card and not just those of participating institutions in a particular system), two or more shared networks can be linked together. Any transaction arriving at the front-end switch that is not for any of the participating institutions is switched to the appropriate network. One configuration for this is shown in figure 4.10. A variation of the front-end switch is shown in figure 4.11.

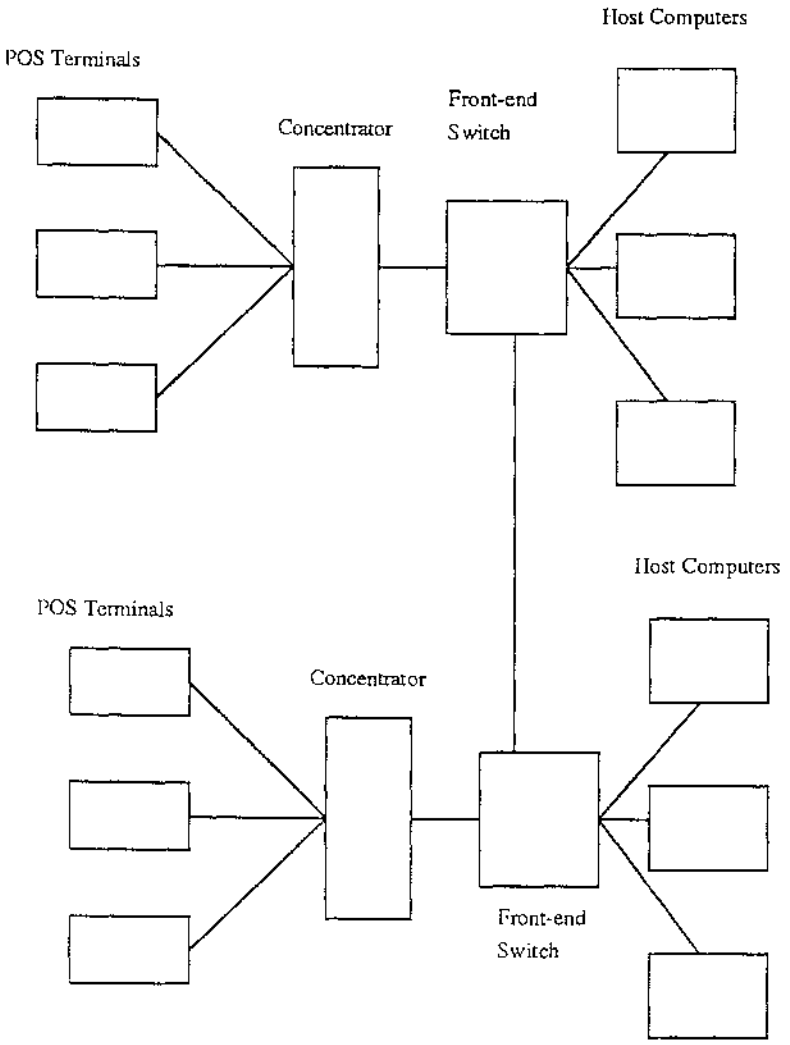


Figure 4.10 Open Access System

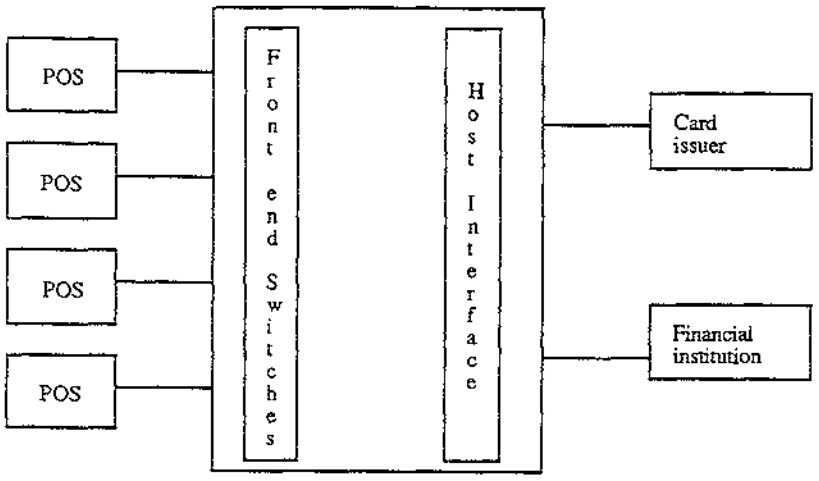


Figure 4.11 Front-end EFTPOS system

Encryption is used to protect PINs in transit. It is not usual practice to encrypt the transaction details but to guarantee the integrity of the data a message authentication code is appended. When DES is used for this purpose, the key has to be available at both ends of the communication line. It depends upon how the network is configured as to what pieces of equipment have to share keys. The following can be paired : the terminal and the acquirer's processor, the terminal and the switch, the switch and the card issuer's bank, the acquirer's and issuer's host processors.

4.3.4 Proposed analysis

An on-line EFTPOS system using either magnetic stripe or smart card technology is analysed in order to determine the security threats. Smart cards have not yet been widely introduced but it seems appropriate to assess the risks since they are likely to be heavily used in the future. It will be assumed that transactions (and PINs when magnetic stripe cards are used) are transmitted to the appropriate computer from a terminal using one or more switches (front-end, central or back-end switch). The probability of a threat occurring at a switch is not considered but obviously the more switches there are in a system the greater the risk.

4.3.5 Conclusion

Table 4.4 identifies all the major risks that apply to EFTPOS. Some of the more significant findings are discussed below. EFTPOS, not surprisingly, has many problems in common with ATM on-line systems. In both cases transactions are entered into a terminal and the customer authenticated by possession of a card and knowledge of a PIN terminal. A terminal, communications component or line, or even the computer may break down causing cardholders and retailers considerable inconvenience. The security of the PIN information is a matter of some concern. It may be discovered at various stages, generation, issuance, processing or storage. Opportunities may also arise for the retailer or his staff to discover both card and PIN information (the installation of dummy terminals for instance). Without encryption and MAC processing, the transmitted transactions and messages from the computer centre can be intercepted or altered by wiretappers. Even when encryption is used, it may be difficult to devise an effective key management scheme when large number of terminals located in retailer's premises are involved.

Other potential attacks include the re-routing of transactions to a dummy host computer which accepts all transactions and returns apparently genuine responses. Software may be manipulated so that retailer credits or customer debits are processed against the wrong account. Sabotage aimed at a particular retailer or the bank itself cannot be ruled out. Finally, two factors make the scale of an EFTPOS operation difficult to control, the number of terminals placed with retailers and the size of the network (probably shared or even joint).

Table 4.4 Principle risks in EFTPOS systems

(The major risks are identified by the use of bold type face)

Chapter 5

5.2	**Disaster to hardware**
5.3.1	Minor disaster
5.3.2	Malfunctioning equipment
5.4	Error
5.5.1	Interference with hardware
5.5.2	Theft of equipment
5.5.3	Extortion
5.5.4	Misuse of computer resources
5.5.5	Vandalism
5.6	**Sabotage**

Chapter 6

6.2	**Disaster**
6.3	Accident
6.4	Error
6.4.1	**Errors in the software lifecycle**
6.4.2	**Omissions**
6.5.1	**Unauthorised change to software**
6.5.1.1	**Program modification to facilitate fraud**
6.5.1.2	**Program modification to cover up fraud**
6.5.1.3	**Circumvention of security controls**
6.5.1.4	Deliberate error
6.5.2	Methods of attack
6.5.3	Copying software
6.5.4	Extortion
6.5.5	Disclosure of software
6.5.6	**Running unauthorised software**
6.5.7	Rerunning, restarting or cancelling jobs improperly
6.5.8	Opportunities
6.6	**Sabotage**

Chapter 7

7.2 Disaster
7.3 Accident
7.4 Errors
7.4.1 Incorrect input
7.4.2 Incorrect processing
7.4.3 Incorrect output
7.4.4 Loss or corruption of data
7.4.5 Omissions
7.5.1 Unauthorised use of passwords
7.5.2 Masquerading as a legitimate customer
7.5.2.1 Cards
7.5.2.2 Discovery of PIN
7.5.3.1 Alteration of data input
7.5.3.2 Alteration of messages
7.5.3.3 Error correction
7.5.3.4 Changing files
7.5.3.5 Data alteration during processing
7.5.3.6 Additional transactions
7.5.4 Collusion
7.5.5 Taking advantage of a genuine error
7.5.6 Falsification of data
7.5.7 Suppression, alteration or destruction of output
7.5.8 Misuse of output
7.5.9 Disclosure of data
7.5.10 Extortion
7.5.11 Denial of valid transaction
7.5.12 Theft of data
7.6 Sabotage

Chapter 8

8.2 Disaster
8.3 Accident
8.3.1 Equipment breakdown or fault
8.3.2 Noise on the line
8.4 Errors
8.4.1 Failure to provide adequate back-up
8.4.2 Insufficient capacity

8.4.3 Poor quality lines
8.4.4 Omissions
8.5.1 Tapping of communication lines
8.5.1.1 Passive wire tap attack
8.5.1.2 Active line tap
8.5.2 Masquerading
8.5.3 Between the lines entry
8.5.4 Browsing
8.5.5 Emulation of equipment
8.5.6 Disclosure of information
8.5.7 Extortion
8.5.8 Attack on network components
8.5.9 Taking advantage of on-going maintenance
8.6 Sabotage
8.7 Risks to encryption and message authentication

Chapter 9

9.2 Disaster
9.3 Accident
9.4 Error
9.4.2 Unusable card
9.4.3 Failure to protect documents
9.5.1 Unauthorised use of sensitive documents
9.5.5 Vandalism
9.5.6 Discrediting an electronic banking service
9.6 Sabotage
9.7.4.1 Retailer problems with EFTPOS
9.7.4 Security
9.7.5 Legal issues
9.7.6 Customer privacy
9.7.8 People

4.4 Credit cards

The bank credit card was first introduced by the Franklin National Bank in 1951 and other banks all over the world soon followed its lead. Today, there are four major credit card companies, Mastercard and Visa in the United States of America, Access (Mastercard's European associate) and Barclaycard (Visa's European associate), as well as a host of minor ones. There are also two very well-known Travel and Entertainment cards, Diner's Club and American Express, which provide monthly credit only. American Express has also introduced the "Optima" card which offers the same facilities as the major credit cards (Hawk,1987). Bank credit cards have been very successful; they can be used in place of cash or cheque as a method of payment to merchants and they sometimes allow the holder to obtain a cash advance from the card-issuing institution. The possession of a card, therefore, serves to identify a customer as a person entitled to unsecured credit from the card issuing financial institution.

4.4.1 Current usage

Instead of paying for a purchase a customer hands over a plastic card. Before completing the transaction the merchant is usually required to check that the transaction can go ahead. Many card issuing institutions have set up authorisation procedures in order to reduce their losses from fraud. If the merchant does not follow the approved procedures, the card issuing institution will not accept any resulting loss. Depending upon the bank's policy, the retailer may have to :

1. Check the card account number against a file of lost or stolen cards.

2. Obtain the approval of the card-issuing institution when a card transaction is above a specified amount. This authorisation process, generally carried out by telephone is time consuming and is not always carried out by staff in retail outlets. In some cases the process is automated, making use of an authorisation telephone .

3. Obtain on-line approval of all transactions via a terminal. In the United States of America, it is estimated that ten to fifteen percent of merchants have a terminal of some type (Goslar,1986).

If the transaction is authorised the card is placed in a device which imprints customer information on the sales draft; the amount of the purchase is written on the draft which is then signed by the customer. Provided the signature corresponds to that on the card, one copy of the voucher is given to the customer as a receipt whilst the other copy is deposited, probably at the end of the day, with the merchant's bank. The merchant's bank usually credits his account immediately with the total value of the sales drafts deposited. It is then the responsibility of the merchant's bank to send all the information to the data processing centre. Both the merchant's bank and the card-issuing service are paid a fee by the retailer for the services they render. Finally the customer receives a monthly statement of account listing all the transactions that have been received since the last billing period. A minimum payment has to be made otherwise a penalty fee is incurred. Interest will be charged on the balance outstanding after payment has been made.

4.4.2 The card issuing institution

The card issuing company has the responsibility for setting up and running the credit card system. As the guarantor of credit it is the card issuing institution that is principally at risk. Credit limits can easily be exceeded by cardholders who do not have the means to repay their debts. Many important decisions need to be taken. Account holders may be routinely supplied with a card or applicants may have to furnish references as to their credit worthiness. The credit limit granted will depend on the circumstances of the customer. For example, students would generally be given a small credit limit. An upper limit per transaction with a merchant must be established. For any purchase or purchases above this amount a retailer should contact the card issuing institution to check whether the cardholder has sufficient credit to allow the sale to proceed. The number of days that

free credit can be enjoyed, the rate of interest then charged and the minimum monthly repayment must all be decided. These have to be changed as necessary, for example when money becomes more expensive to borrow.

4.4.2.1 Plastic card

Currently the customer name, account number and expiry date are embossed on the card and also stored on the magnetic stripe. Magnetic stripe technology which has been described in section 3.6.1 became a standard feature on cards in 1982 and allows credit cards to be used in automated systems via an EFTPOS terminal or an ATM. Smart card technology is also being exploited. Mastercard has made a definite commitment to introduce the integrated circuit card following successful field tests (Ladouceur,1987) whilst Visa, in conjunction with Toshiba, has just announced the world's first "supersmart" card. This card incorporates both a micro-computer and a calculator-like keyboard. Other features include a liquid crystal display at the back and a built-in battery (Dominion, 1988).

Credit cards that carry a microelectronic chip can be used in conjunction with EFTPOS terminals to cut out all movement of paper, provide for the electronic transmission of data and allow off-line authorisation of the transaction (Brown and Brown,1986). In this "store and forward" system (See figure 4.12), when the smart card is inserted into the special reader various checks can be made. The terminal is able to consult its current list of stolen or withdrawn cards and the processor on the smart card checks that the PIN entered at the terminal is the same as that of the cardholder. Moreover, since the smart card allows the customer's credit limit to be stored in its memory, this information can be accessed to check that the current purchase does not exceed this amount. If the purchase is authorised then the transaction details are stored by the terminal for sending to the bank's computer and written to the memory of the smart card which automatically debits the credit limit. After payments to the card-issuing institution this credit limit can be refreshed by inserting the card in an ATM.

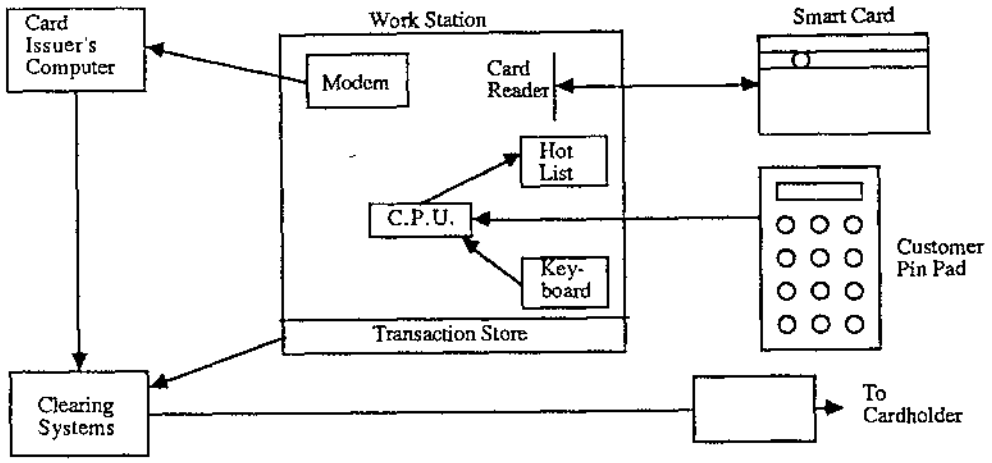


Figure 4.12 Store and forward system (Brown and Brown,1986)

4.4.3 Proposed analysis

A typical credit card system is assumed for the purposes of this thesis. Those retailers who do not have terminals make an authorisation check for high value purchases by telephone. Computers are used in this context for processing transaction details. Since smart cards will soon be used widely to ensure that customers do not exceed their limit, it is essential to consider the risks to them as well as the threats to the magnetic stripe card.

4.4.4 Conclusion

Table 4.5 identifies the major risks that apply to all credit cards. Transactions cannot be processed in the event of a disaster to the computer or the support facilities. Cards can be counterfeited or the file of lost or stolen card numbers altered to allow a fraud to proceed. A programmer may change software so that when the monthly statements are produced certain purchase transactions (of friends perhaps) are not processed.

The risks to magnetic stripe credit cards are shown in table 4.7. The two greatest threats currently are fraud and bad debt; the combined loss from these is considerable. Credit

card fraud can take place at every stage of the transaction. Customers are identified by a card and signature but counterfeit cards can be used or unsigned credit cards obtained. Merchants can also cheat the bank by sending sales drafts for non-existent purchases. The database of records can be altered so that a credit limit is raised. Bad debt occurs because customers buy more goods than they can pay for, deliberately exceeding the card's limit in many cases.

Smart cards prevent the total credit line from being advanced and provide for more secure identification of the customer. As with all systems that use PINs, however, this information can be obtained by other people. The use of communication systems makes a store and forward system vulnerable to an equipment failure. The problem also arises that transaction information may be lost during a breakdown and the only copy may be stored on the customer's card. Key management is a problem if encryption is used. The smart card appears to be less durable than a card with only a magnetic stripe. These risks are summarised in table 4.7.

Table 4.5 Principle risks in all credit cards systems

(The major risks are identified by the use of bold type face)

Chapter 5

5.2	**Disaster to hardware**
5.3.1	Minor disaster
5.3.2	Malfunctioning equipment
5.4	Error
5.5.1	Interference with hardware
5.5.2	Theft of equipment
5.5.3	Extortion
5.5.4	Misuse of computer resources
5.5.5	Vandalism
5.6	**Sabotage**

Chapter 6

6.2 Disaster
6.3 Accident
6.4 Error
6.4.1 Errors in the software lifecycle
6.4.2 Omissions
6.5.1 Unauthorised change to software
6.5.1.1 Program modification to facilitate fraud
6.5.1.2 Program modification to cover up fraud
6.5.1.3 Circumvention of security controls
6.5.1.4 Deliberate error
6.5.2 Methods of attack
6.5.3 Copying software
6.5.4 Extortion
6.5.5 Disclosure of software
6.5.6 Running unauthorised software
6.5.7 Rerunning, restarting or cancelling jobs improperly
6.5.8 Opportunities
6.6 Sabotage

Chapter 7

7.2 Disaster
7.3 Accident
7.4 Errors
7.4.1 Incorrect input
7.4.2 Incorrect processing
7.4.3 Incorrect output
7.4.4 Loss or corruption of data
7.4.5 Omissions
7.5.1 Unauthorised use of passwords
7.5.2 Masquerading as a legitimate customer
7.5.2.1 Cards
7.5.2.1.1 Counterfeit cards
7.5.2.1.2 Fraudulent application for a card.
7.5.2.1.4 Use of lost or stolen cards
7.5.2.1.5 Alteration of cards
7.5.2.1.6 Fraudulent charges by merchants

7.5.2.2	**Discovery of PIN**
7.5.3.1	**Alteration of data input**
7.5.3.2	**Alteration of messages**
7.5.3.3	Error correction
7.5.3.4	**Changing files**
7.5.3.5	**Data alteration during processing**
7.5.3.6	**Additional transactions**
7.5.4	**Collusion**
7.5.5	**Taking advantage of a genuine error**
7.5.6	Falsification of data
7.5.7	Suppression, alteration or destruction of output
7.5.8	Misuse of output
7.5.9	**Disclosure of data**
7.5.10	**Extortion**
7.5.11	**Denial of valid transaction**
7.5.12	**Theft of data**
7.6	**Sabotage**

Chapter 9

9.2	**Disaster**
9.3	Accident
9.4	Error
9.4.3	Failure to protect documents
9.5.1	**Unauthorised use of sensitive documents**
9.5.5	**Vandalism**
9.5.6	Discrediting an electronic banking service
9.6	**Sabotage**
9.7.4	**Security**
9.7.5	**Legal issues**
9.7.6	**Customer privacy**
9.7.8	**People**

Table 4.6 Additional risks to magnetic stripe credit cards

7.5.2.1.3	**Obtaining an unsigned card**
7.5.2.1.7	**Mail order and telephone fraud**
7.5.2.1.8	**Use of returned or captured cards**
9.7.2	**Credit card losses**

Table 4.7 Additional risks to smart cards

7.5.2.2	**Discovery of PIN**
7.5.3.2	**Alteration of messages**
8.2	**Disaster**
8.3	Accident
8.3.1	Equipment breakdown or fault
8.3.2	Noise on the line
8.4	Errors
8.4.1	**Failure to provide adequate back-up**
8.4.2	**Insufficient capacity**
8.4.3	Poor quality lines
8.4.4	Omissions
8.5.1	Tapping of communication lines
8.5.1.1	**Passive wire tap attack**
8.5.1.2	**Active line tap**
8.5.2	**Masquerading**
8.5.3	**Between the lines entry**
8.5.4	**Browsing**
8.5.5	**Emulation of equipment**
8.5.6	Disclosure of information
8.5.7	**Extortion**
8.5.8	**Attack on network components**
8.5.9	**Taking advantage of on-going maintenance**
8.6	**Sabotage**
8.7	**Risks to encryption and message authentication**

4.5 Home banking

Through technological advances customers are now able to communicate directly with a bank from their own home via a terminal of some kind and using dial-up or packet-switching facilities. The term home banking encompasses the many services - funds transfer, balance enquiry etcetera - that can be offered in this way. Historically the first step in this process was the introduction of telephone bill payments (TBP) in the United States in the 1970s. This funds transfer facility permits customers to pay bills. By phoning their financial institution, authorizing it to debit their account and specifying the names of all those to whom payments should be made, a customer can pay several bills at once. TBP is obviously limited in its scope and video home banking is now seen as providing a full range of services. Home banking facilities are available world-wide. The pioneer in this area was the Nottingham Building Society in conjunction with the Bank of Scotland. Other services include Covidea (the joint venture of Bank of America and Chemical Bank) in the United States, Telebank in Australia and Teledata in New Zealand.

4.5.1 Videotex

At the heart of home banking is the videotex system. Videotex is the term used by the International Telephone and Telegraph Consultative Committee to describe the technology needed to deliver home information services electronically. The first videotex system "Prestel", introduced by the British Post Office (now known as Telecom) in 1976, allowed consumers to access a database to find out about the weather forecast, stock exchange prices, etcetera by using an adapted television, telephone connection and a keypad. Initially seen as an information retrieval service, it was soon realized that videotex had the potential to provide an on-line real time capability for customers. To set up transaction services the following elements must be available (Good,1983) :

1. Hardware

Information can either be typed into a terminal (a personal computer, adapted television or special purpose videotex terminal is typically used) or spoken into a telephone. A modem may be required, depending on the nature of the communications link. Unless a special purpose terminal is used, a decoder has to be connected to the modified television or personal computer to receive the information and display it on the screen.

2. System Operator

The operator of the videotex system must be able to connect up consumers to the organisation of their choice by providing appropriate networking facilities. This is a two stage process. The consumer sends a request in the first instance to the system operator's computer which then sets up the connection with the desired host. The data is transmitted to and from the computer of the consumer's choice either by telephone, cable, satellite or a combination of these alternatives. Given the fact that the telephone is a national switching system, it is usual for a dial-up connection to be set up between the customer and the system operator. Subsequently, packet switching techniques or a dedicated line can be used to access the service provider. This network is known as a "gateway" system. The system operator obviously has a controlling function. Such matters as terminal connection, provision of the hardware and software, usage recording and billing are managed at this point.

3. Information Provider

An information provider fulfils the need for retrieval of information on topics such as the weather, the news, financial quotes and entertainment listings.

4. Service provider

The service provider offers the consumer various facilities, transactional (home banking and shopping), computing (added storage and processing power to microcomputers) and messaging (electronic mail). It will depend on a particular system whether or not both services and information are supplied. Such a system appears in figure 4.13.

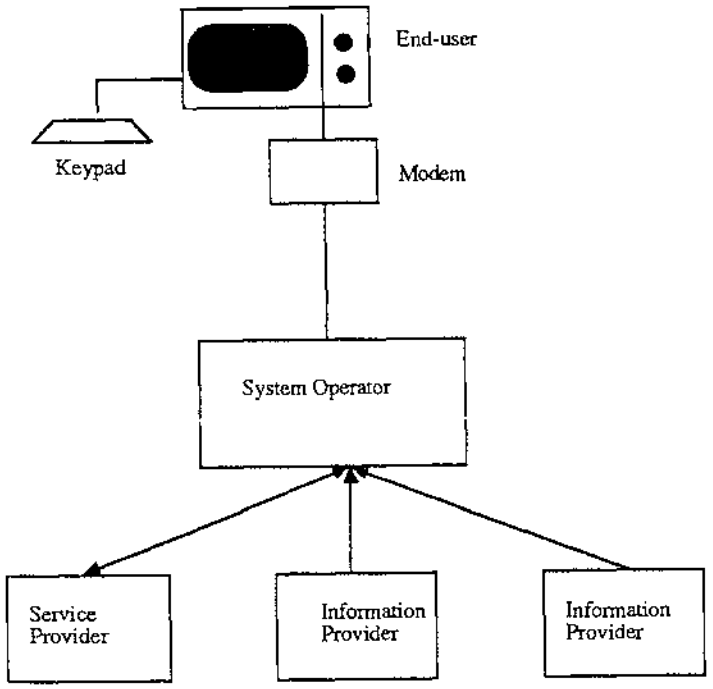


Figure 4.13 Videotex system

4.5.2 Home banking services

Using the videotex technology described above, home banking is now gaining a foothold in many countries of the world. The term is not only used to describe the services offered to an individual in his own home but also to businessmen. Many options are available depending on the system to which a customer subscribes and the amount of money he is prepared to pay .

1. Retrieval of account details.

An essential home banking service is the ability to provide a customer with the balance of an account. Additionally, statement details may also be made available.

In Australia, any Telebank subscriber with a printer can obtain hard copy from a screen.

2. Transaction Processing.

Money can be transferred between a customer's accounts, cheque, savings, loan and credit card. Payments can also be made to third parties automatically and cheques written.

3. Ordering

A customer is able to request a statement or a cheque book to be sent.

4. Retrieval of Financial Information.

This service is generally made use of by organisations but can still be obtained by an individual. Covidea provides 'Investment Edge' a stock brokerage, portfolio management and market information service. Telebank, running in Australia, allows subscribers to monitor movements in interest rates domestically and to view regularly updated foreign exchange rates.

5. Electronic Mail.

Messages can be transmitted to customers along the communications link. Lipis (1985) suggests that confirmation or denial of a loan application can be sent in this way.

6. Home Budgeting.

A budgeting service is provided which allows the computer to make the necessary calculations. Computational power is also required.

7. Cash Management.

Cash management modules give the business man fast access to relevant information. The Bank of Scotland's package provides:

- The opening ledger balance each day
- The cleared balance
- A detailed breakdown of items that have been received by the bank and will be cleared that day.

A very useful software package was made available by the Bank of America in November 1985. Customers can combine their cheque account and savings account records with their home, business and tax information.

4.5.2.1 Systems Operation

Lipis (1985) identifies four major operational requirements in a home banking system.

(1) Customer Information Preparation

Information has to be available to identify customers. The relevant account information will also be required.

(2) Network control

Hardware and software is necessary to control incoming calls, maintain the telephone line protocol, control the audio response unit and route messages to and from customers.

(3) Session management

Software has to direct a customer through the session, prompt the customer to enter transactions and capture customer entered transactions.

(4) After session transaction processing

Transactions must subsequently be processed against customer accounts. Payments to non-customers must also be dealt with.

4.5.3 Proposed analysis

A bank may choose to provide all or some of the functions just described. A bank may set up its own network, co-operate with a common carrier who offers no other videotex services or co-operate with a common carrier who offers other videotex services as well as home banking. In the last case, if many financial and non-financial institutions are connected by such a network operator then the danger from a security viewpoint is at its greatest since the bank's database is potentially accessible to many different users. Moreover, the bank cannot control admission to the videotex system. Consequently, it is this case where the bank performs customer information preparation, session management and after session transaction processing that will be examined in this thesis. (See figure 4.14).

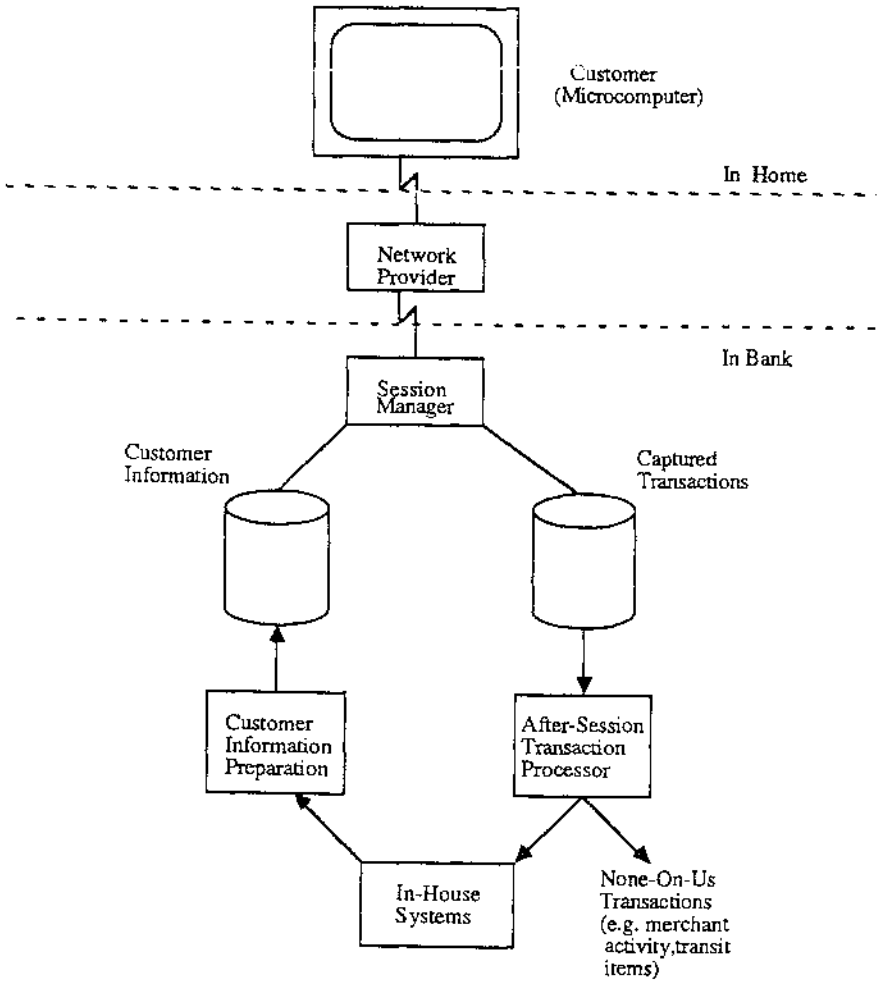


Figure 4.14 Home Banking System

The network is operated independently and a customer has in the first place to sign on to the videotex system. From the various services offered, the consumer will then select the home banking option. The bank takes over from this point, prompting the customer by means of menus through the home banking services. The customer will be requested to enter an account number and password before choosing from the listed alternatives. All the information relevant to a transaction has then to be captured. For example if the bill-paying alternative is chosen, the account number of the payee and the amount due have to be input by the customer. The bank controls the proceedings until the customer indicates that he has finished. When the customer finishes home banking then the system operator takes over again. The bank, of course, may still have to make a payments to a merchant. To date encryption is not generally used in home banking because of the problems and costs involved with installing encryption devices at both ends of the line.

4.5.4 Conclusion

Table 4.8 identifies all the major risks that apply to home banking. Some of the more significant findings are discussed below. The authentication of the customer is again a major security risk. The customer account number and PIN at least are are required to operate an account and these can be obtained by anyone tapping a telephone line. Further levels of security are usually built in but it is possible that they may be discovered by bank employees or family members. It should be noted that if the customer selects or is given the same PIN for the home banking, EFTPOS and ATM application, it can be discovered by passive wiretapping and used to defraud the bank at a later date.

It is also possible to connect a computer to the line and alter transactions that are being transmitted. The customer and bank still believe that they are in communication with each other but they are actually receiving information from the perpetrator. In this way, it is possible for a criminal to transfer money from the customer's account to his own. A credit can also be made to the wrong account as a result of a software errors or unauthorised changes. Finally, a hacker may be able to use his computer to bypass the

computer's access controls and alter the stored data. In this way he could, for instance, increase his balance.

Table 4.8 Principle risks in home banking systems

(The major risks are identified by the use of bold type face)

	Chapter 5
5.2	**Disaster to hardware**
5.3.1	Minor disaster
5.3.2	Malfunctioning equipment
5.4	Error
5.5.1	Interference with hardware
5.5.2	Theft of equipment
5.5.3	Extortion
5.5.4	Misuse of computer resources
5.5.5	Vandalism
5.6	**Sabotage**

	Chapter 6
6.2	**Disaster**
6.3	Accident
6.4	Error
6.4.1	**Errors in the software lifecycle**
6.4.2	**Omissions**
6.5.1	**Unauthorised change to software**
6.5.1.1	**Program modification to facilitate fraud**
6.5.1.2	**Program modification to cover up fraud**
6.5.1.3	**Circumvention of security controls**
6.5.1.4	Deliberate error
6.5.2	Methods of attack
6.5.3	Copying software
6.5.4	Extortion
6.5.5	Disclosure of software
6.5.6	**Running unauthorised software**
6.5.7	Rerunning, restarting or cancelling jobs improperly
6.5.8	Opportunities
6.6	**Sabotage**

Chapter 7

7.2	**Disaster**
7.3	Accident
7.4	**Errors**
7.4.1	**Incorrect input**
7.4.2	**Incorrect processing**
7.4.3	**Incorrect output**
7.4.4	**Loss or corruption of data**
7.4.5	**Omissions**
7.5.1	Unauthorised use of passwords
7.5.2	**Masquerading as a legitimate customer**
7.5.2.3	**Home banking**
7.5.3.1	**Alteration of data input**
7.5.3.2	**Alteration of messages**
7.5.3.3	Error correction
7.5.3.4	**Changing files**
7.5.3.5	**Data alteration during processing**
7.5.3.6	**Additional transactions**
7.5.4	**Collusion**
7.5.5	**Taking advantage of a genuine error**
7.5.6	Falsification of data
7.5.7	Suppression, alteration or destruction of output
7.5.8	Misuse of output
7.5.9	**Disclosure of data**
7.5.10	**Extortion**
7.5.11	**Denial of valid transaction**
7.5.12	**Theft of data**
7.6	**Sabotage**

Chapter 8

8.2 Disaster
8.3 Accident
8.3.1 Equipment breakdown or fault
8.3.2 Noise on the line
8.4 Errors
8.4.1 Failure to provide adequate back-up
8.4.2 Insufficient capacity
8.4.3 Poor quality lines
8.4.4 Omissions
8.5.1 Tapping of communication lines
8.5.1.1 Passive wire tap attack
8.5.1.2 Active line tap
8.5.2 Masquerading
8.5.3 Between the lines entry
8.5.4 Browsing
8.5.5 Emulation of equipment
8.5.6 Disclosure of information
8.5.7 Extortion
8.5.8 Attack on network components
8.5.9 Taking advantage of on-going maintenance
8.6 Sabotage

Chapter 9

9.2 Disaster
9.3 Accident
9.4 Error
9.4.3 Failure to protect documents
9.5.1 Unauthorised use of sensitive documents
9.5.6 Discrediting an electronic banking service
9.6 Sabotage
9.7.4 Security
9.7.5 Legal issues
9.7.6 Customer privacy
9.7.8 People

4.6 Wire Transfers

A wire transfer can be used to effect speedy payment of funds from a remitter to a beneficiary. A telecommunications network is necessary to support this fast movements of funds. Wire transfers have become increasingly popular as institutions make payments as late as possible on the one hand and collect funds as soon as possible on the other. This allows them to maximize the earning of interest on monies in their possession. In the United States of America Fed Wire, Telex and Chips are available; in the UK Chaps has been set up and internationally, SWIFT can be used. These systems deal with millions of dollars each day. It has been estimated that in the United States US$3 trillion dollars flow weekly through the many automated payment systems (Cline,1986)

4.6.1 Functions of a wire transfer system

Electronic payments of many kinds can be made using wire transfer systems : transmission of funds transfer and payment instructions, transfer of funds and securities, cash withdrawals, loan advances and direct deposits. The flow of messages through a wire transfer service is illustrated in figure 4.15. There are three principle functions (Lipis,1985) :

1. Payment Ordering

   A party such as a bank, corporate customer or an individual decides to make a payment. Instructions are then given to the bank to initiate the wire transfer. At this point, verification of the message must take place otherwise a fraudulent transaction may be permitted. The method of authentication will depend on the means used to transmit instructions - telephone, telex, TWX, wire service, facsimile, mail. Answer back systems, test keys and passwords are used as appropriate.

2. Payment Processing and Delivery

   The funds are transferred through a wire transfer network. It is usual to employ two operators at this point - one to enter the instructions into the funds transfer

network and the other to check that this has been performed correctly. Similarly on receipt of the transfer of funds information, one operator acknowledges its arrival whilst the other balances the accounts. The two banks concerned in a transaction have to agree on a method of authentication: a test key known only to the parties concerned is usually included in the message.

3. Payment Advising

On receipt of the data, the beneficiary is advised that the funds transfer has been effected. The funds may or may not be made available on the day of arrival.

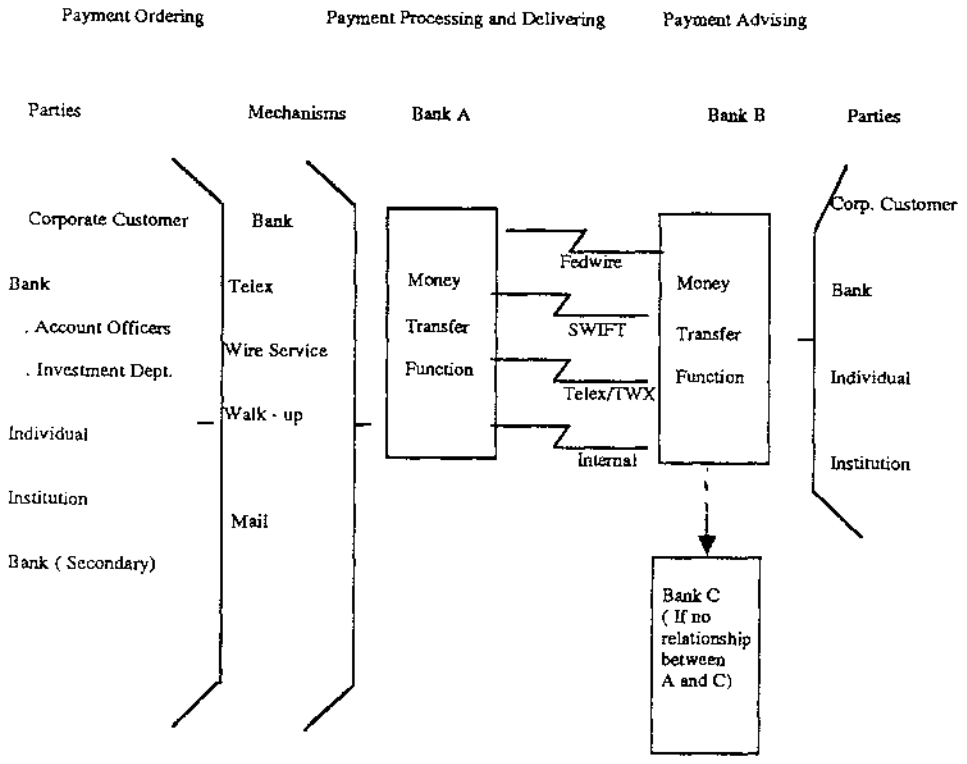


Figure 4.15 Wire transfer system (Lipis,1985)

4.6.2 Operation

Two separate flows of information are involved in processing a wire transfer. In the first place full details about the transaction must be captured. Secondly, the funds involved have to be transferred to the beneficiary. The flow of information through a network can be quite complex. The following two examples for a domestic wire transfer and an international wire transfer taken from Lipis (1985) illustrate this (figures 4.16 and 4.17 respectively).

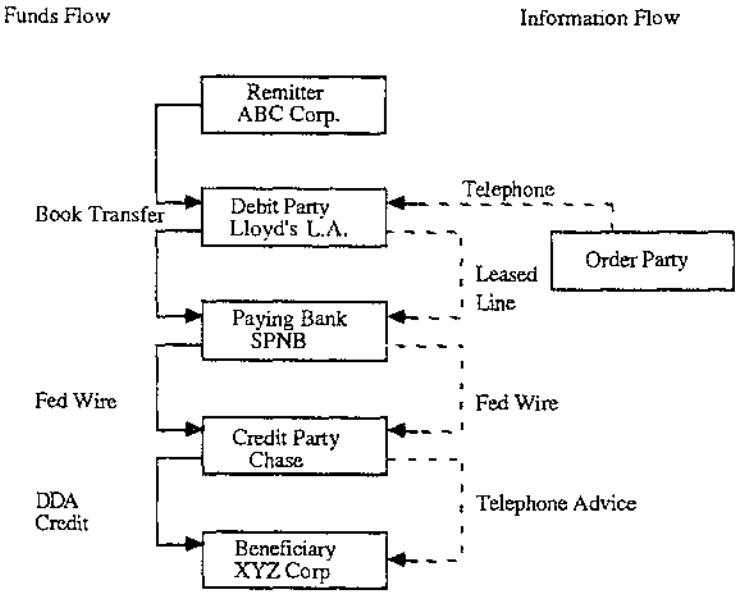


Figure 4.16 Domestic wire transfer (Lipis,1985)

4.5.2.1 Domestic transfer

The sequence of events in a Domestic Wire Transfer between the ABC Corporation and XYZ Corporation is as follows:

1. ABC Corporation telephones instructions to its bank, Lloyds of Los Angeles to transfer funds to XYZ Corporation bank Chase Manhattan in New York.
2. Lloyds charges the account of ABC and transmits the order to security Pacific. A bank transfer is then made between Lloyds and Security Pacific.
3. Security Pacific makes use of the Fed Wire network to transfer funds to Chase Manhattan.

4. Chase Manhattan credits XYZ's account and advises the XYZ Corporation of the transfer.
5. Security Pacific informs Lloyds of the transfer.
6. Lloyds notifies ABC Corporation that the funds have been transferred.

4.6.2.2 International transfer.

An International Transfer where ABC Corporation in San Francisco obtains funds from its Berlin Office proceeds as follows:

1. ABC Corporation in San Francisco (with an account at Lloyds) sends a telex to its bank in Berlin (a branch of Deutschbank) asking for funds to be remitted.
2. The branch notifies ABC, Berlin of this transfer and transfer the funds to the bank's head office in Frankfurt.
3. The Frankfurt branch of Deutschbank notifies Citibank in New York via SWIFT of the funds transfer and a book transfer of the funds is effected.
4. Citibank makes a transfer to Security Pacific's head office in Los Angeles.
5. Security Pacific makes an interoffice accounting entry and notifies Lloyds of Los Angeles. Lloyds is credited with the funds.
6. Lloyd's of Los Angeles makes an interoffice settlement with Lloyds of San Francisco.
7. Lloyds of San Francisco notifies ABC, San Francisco, that the transfer is completed.

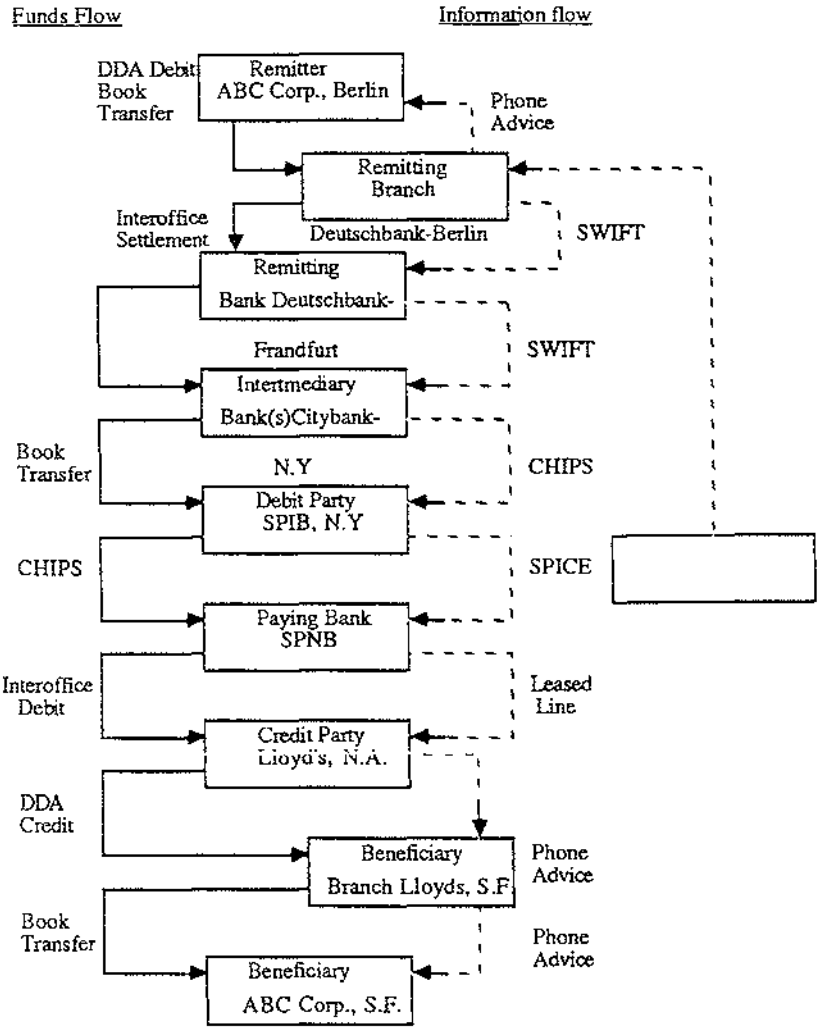


Figure 4.17 International wire transfer (Lipis,1985)

It should be noted that not all pairs of banks can communicate directly and a bank often has to make use of intermediaries to act on its behalf. With regard to international transfers, pairs of banks specialize in this service, offering it in competition with other banks. The communication components of wire transfer systems are not described in detail as they are basically the same as those used in ATM and EFTPOS systems. As described in section 3.4.3, messages can be encrypted in order to protect them during transmission. This is considered advisable in view of the large sums involved.

4.6.3 Funds transfer systems

There are many wire transfer systems but three will be described. These have been chosen to illustrate different ways in which the settlement of funds between banks takes place. This issue is of great concern to those using wire transfer systems since if not handled properly a bank (or banks) might become bankrupt.

1. Society for Worldwide Interbank Financial Telecommunications (SWIFT)

   Internationally, the Society for Worldwide Interbank Telecommunications (SWIFT) is used for moving money between banks. Access to SWIFT is controlled by a log-in system that requires a different password for every message transmission session. Whilst data is encrypted on the SWIFT network (using a secret algorithm), there is no requirement for banks to encrypt messages before entry to the SWIFT network at a regional processor. Messages though also carry an authentication code that allows the receiving bank to verify that the message delivered is the one that was originally sent. SWIFT accepts the responsibility only for the transmission of messages; it is left up to the banks to handle settlement. The receiving bank debit's the sender's account and credits the beneficiary's. The receiving bank may give credit to a beneficiary pending settlement from the sending bank at its discretion. SWIFT II with its increased capacity and support for new network products has been promised for years. It will not be operative, however, until at least the second quarter of 1988 (Church,1987). It should be noted that SWIFT II will make only minor changes to its security procedures because of satisfaction with existing measures.

2. Fed Wire

   Fed Wire, owned by the government of the United States of America, settles transactions immediately that is once a customer has been advised of the transfer, the funds are also made available to him. Those banks that end the day with an overdraft cover their position by purchasing funds from the Federal Reserve Bank. With the repayment of those funds early the next morning, the banks

concerned have a daylight overdraft again (ABA Journal,Sept 1986). The Federal Reserve Bank was so concerned about the possible failure of a bank that limits were set on the size of the overdraft that could be incurred. The formula is related to the bank's capital and is often referred to as a "cap". Further details about "caps" are given in section 9.7.3.

3. Clearing House Interbank Payment Systems (CHIPS)

Clearing House Interbank Payment Systems (CHIPS) delays settlement until the end of a business day, netting out the transactions so that one payment is sufficient to settle all the day's business. A bank may credit the receiver's account at the end of the business day after settlement has taken place or give immediate credit if it so wishes. CHIPS, which handles mainly overseas payments, is able to monitor the current position of the member banks (ABA Journal,Sept 1986). Once a bank reaches its overdraft limit the CHIPS computer will not allow any further payments to be made.Moreover each bank determines how much credit it will allow another bank. There is still no receiver finality in CHIPS, however, since this does not happen until CHIPS settles through the Federal Reserve Bank at the end of the day. There is always the possibility that at the end of the trading day, a bank cannot cover its debit position. CHIPS has three options open to it at this point. The first possibility is to delay payment, the second is to discard all the transactions of the failed bank from the network and the third is to reverse all of the day's transactions. The possibility, however remote, that all transactions could be unwound reduces confidence in the system. Any private-sector payment system could face very serious problems if a bank failed during a day's trading.

4.6.4 Proposed analysis

Whilst wire transfer systems do differ in detail, they all work essentially in the same way - incoming message, transfer of message, receipt of message. No specific funds transfer system will be looked at but this general case will be considered. The additional risk borne by the same day settlement systems will be mentioned where necessary.

4.6.5 Conclusion

Of all the services considered in this thesis, wire transfer is most at risk as it involves the speedy transfer of vast sums of money daily. Indeed, no wire transfer system can succeed unless individuals and corporations have confidence that it is secure, reliable and respects their privacy. There are several threats to be countered. A hardware or communications failure can lead to a slow down or temporary loss of service which delays payments, causing liquidity problems to banks and customers alike. A saboteur who wishes to attack the capitalist nations can damage a network so that it is put out of commission for several days. An error can easily be made; the inadvertent alteration, misdirection or duplication of a funds transfer may result in the recipient absconding with the funds. The danger of fraud is highly likely when the rewards are so high. An unauthorised transfer request can be introduced into the system or the details of a message altered either by staff or wiretappers. Confidential information may also be obtained by passive wiretapping. If encryption is used to protect messages, the need to keep the keys secret is vital. Finally, the consequences of one bank failing can be very serious in a network, causing others in their turn to become bankrupt.

Table 4.9 Principle risks in wire transfer systems

(The major risks are identified by the use of bold type face)

Chapter 5

5.2	**Disaster to hardware**
5.3.1	Minor disaster
5.3.2	Malfunctioning equipment
5.4	Error
5.5.1	Interference with hardware
5.5.2	Theft of equipment
5.5.3	Extortion
5.5.4	Misuse of computer resources
5.5.5	Vandalism
5.6	**Sabotage**

Chapter 6

6.2	**Disaster**
6.3	Accident
6.4	Error
6.4.1	**Errors in the software lifecycle**
6.4.2	**Omissions**
6.5.1	**Unauthorised change to software**
6.5.1.1	**Program modification to facilitate fraud**
6.5.1.2	**Program modification to cover up fraud**
6.5.1.3	**Circumvention of security controls**
6.5.1.4	Deliberate error
6.5.2	Methods of attack
6.5.3	Copying software
6.5.4	Extortion
6.5.5	Disclosure of software
6.5.6	**Running unauthorised software**
6.5.7	Rerunning, restarting or cancelling jobs improperly
6.5.8	Opportunities
6.6	**Sabotage**

Chapter 7

7.2 Disaster
7.3 Accident
7.4 Errors
7.4.1 Incorrect input
7.4.1.2 Erroneous wire transfer
7.4.2 Incorrect processing
7.4.3 Incorrect output
7.4.4 Loss or corruption of data
7.4.5 Omissions
7.4.5.1 Negligence by staff at the sender bank
7.4.5.2 Negligence by staff at the receiving bank
7.5.1 Unauthorised use of passwords
7.5.2 Masquerading as a legitimate customer
7.5.2.4 Wire transfer abuse
7.5.2.4.1 Fraud by an employee of the customer
7.5.2.4.2 Fraud by outsiders
7.5.2.4.3 Fraud by staff at the sending or receiving bank
7.5.2.4.4 Staff employed by the wire transfer system
7.5.3.1 Alteration of data input
7.5.3.2 Alteration of messages
7.5.3.3 Error correction
7.5.3.4 Changing files
7.5.3.5 Data alteration during processing
7.5.3.6 Additional transactions
7.5.4 Collusion
7.5.5 Taking advantage of a genuine error
7.5.6 Falsification of data
7.5.7 Suppression, alteration or destruction of output
7.5.8 Misuse of output
7.5.9 Disclosure of data
7.5.10 Extortion
7.5.11 Denial of valid transaction
7.5.12 Theft of data
7.6 Sabotage

Chapter 8

8.2 Disaster
8.3 Accident
8.3.1 Equipment breakdown or fault
8.3.2 Noise on the line
8.4 Errors
8.4.1 Failure to provide adequate back-up
8.4.2 Insufficient capacity
8.4.3 Poor quality lines
8.4.4 Omissions
8.5.1 Tapping of communication lines
8.5.1.1 Passive wire tap attack
8.5.1.2 Active line tap
8.5.2 Masquerading
8.5.3 Between the lines entry
8.5.4 Browsing
8.5.5 Emulation of equipment
8.5.6 Disclosure of information
8.5.7 Extortion
8.5.8 Attack on network components
8.5.9 Taking advantage of on-going maintenance
8.6 Sabotage
8.7 Risks to encryption and message authentication

Chapter 9

9.2 Disaster
9.3 Accident
9.4 Error
9.4.3 Failure to protect documents
9.5.1 Unauthorised use of sensitive documents
9.5.6 Discrediting an electronic banking service
9.6 Sabotage
9.7.3 Bankruptcy in wire transfer systems
9.7.4 Security
9.7.5 Legal issues
9.7.6 Customer privacy
9.7.8 People

Chapter 5

Threats to Hardware

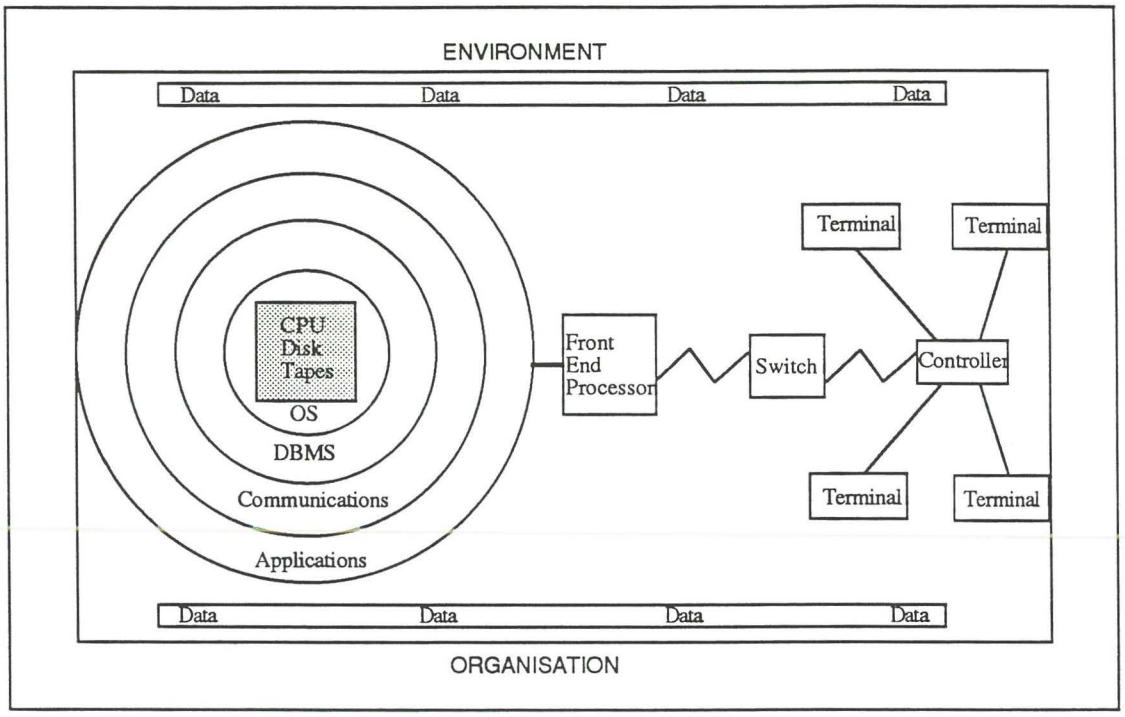


Figure 5.1 Hardware

5.1 Introduction

In this chapter, the threats to hardware are identified under the headings of disaster, accident, error, computer abuse and sabotage. It is assumed that in the computer centre, there will be the host computer(s), printers, disk and tape drives, operator consoles, input devices and data storage media. The data storage media may include on-line devices such as drums and disks as well as the disks and tapes in the library. Communications equipment has its own special problems and these are dealt with in chapter 8. The principle threats to hardware include natural and man-made disasters, malfunctioning of equipment and sabotage.

5.2 Disaster to hardware

A disaster to hardware may be defined as an event that causes such severe damage to the computer installation that it brings operations to a halt. Data and software since they are stored on disk and tape may also be destroyed in such circumstances. This is incidental to the risks to hardware, however, and is dealt with in the appropriate chapters. The types of hazards that occur include the following : fire, flood, lightning, earthquakes, hurricanes, storms, radio-frequency interference, structural failure, power surge and gas explosion. According to some experts fire is the worst single disaster affecting computer-based systems (Bequai,1987). An extended power cut, too, for whatever reason, can have a devastating effect on operations, holding processing up until it is restored. Man made disasters can have equally disastrous consequences; civil riots, incompetence and industrial action can all put the computing system out of action. (Lane 1985). Whilst damage to the computing equipment occurs in these cases by accident rather than design, sabotage from either inside or outside the organisation is a deliberate threat. This issue is considered further in section 5.6. Without off-site back-up facilities a disaster will force an organisation to halt its operations. Even if a contingency plan has been drawn-up, tested and put into operation, the delays incurred can be very serious in electronic banking which relies greatly on the timely processing of data. American studies indicate that a bank would be out of business if a shut down lasted four days (Jaben,1986).

Examples

1. On 9 August 1977 a boiler exploded beneath the computer room of the British firm Bowater Scott. The computer centre was virtually destroyed and the two mainframes damaged but at least the company had back-up files stored off-site. Another company offered time on their machines so that processing was only held up for a short time. Within 15 days, a new computer suite was set up with one of the computers restored and the other replaced (Hayward and Kemp,1987).

This example illustrates the problems that arise following a disaster. The situation is likely to be worse in New Zealand where another company is unlikely to have spare capacity. Moreover a delay of 15 days is too long in electronic banking. Unfortunately, it will take a minimum of five days to get another machine installed even if a suitable computer is available in Australia or the United States and that might be too late.

2. When the National Library in Canberra caught fire, the computer centre remained standing. Unfortunately smoke had been pumped through the air conditioning into the computer room whilst water also seeped in. The computer room was covered in soot, water seepage under the floor destroyed cables, the mainframe was badly damaged by smoke and water, and grease from the clogged pipes of the fire-suppressing gas systems covered the computer. Information stored on the disks could easily be replaced with off-site copies but there was no alternative site immediately available. After three weeks the library was able to start operations again with a borrowed computer in accommodation provided by the Bureau of Statistics (Rydges,1987)

5.3 Accident

5.3.1 Minor disaster

Should any of the hazards described above occur on a small scale (fire that destroys storage media, for example), limited damage to components of the system may cause a temporary loss of service. The Bank of New Zealand's computers were put out of action for two hours because of a power surge that affected the central processing units (Dominion, 1987a). Processing of Visa card transactions was halted and some information in the processing queue was lost.

5.3.2 Malfunctioning equipment

From time to time equipment may be defective or even fail. Three issues that arise from this are the operational reliability of the system, the integrity of the stored data and effectiveness of hardware security controls.

Generally speaking, provided a faulty component is repaired or replaced quickly this is a minor inconvenience from an operational point of view. This is not the case though when there is a lengthy delay, over the CPU for instance. The central processing unit is usually so sophisticated that it can detect and correct most errors. Occasionally, though, a malfunction results in the computer going down with a temporary halt in service. In on-line ATM systems, it is customary to switch then to the less secure off-line mode. Processing may be halted for EFTPOS and home banking. Whilst such a failure is usually inconvenient and may result in bad publicity for a bank, it can have serious consequences in wire transfer systems. At best the result may be the unplanned transfer of processing to other payment systems. At worst the volume of transactions that subsequently has to be processed after recovery may overload the system. Funds for customers will then delayed, deadlines for processing transactions have to be extended and final settlement for the day between the participants may have to be put back. The participants may have to sustain intraday and possibly overnight overdrafts, delays in accounting and customer reporting and disruption of the management of their funds

position. The most serious risk is that a financially sound bank will have, through no fault of its own, liquidity problems that lead to bankruptcy.

Data is stored on devices such as tape and disk as well as being kept temporarily in main memory. If there is a disk head crash all the data stored on the device may be lost. It can only be recovered if it is backed up elsewhere. Unfortunately, the integrity of the data can also be attacked in a more subtle fashion. A hardware fault can result in unexpected changes to the information stored in main memory - either data or software. This may not be noticed at the time and either incorrect records are written back to disk or program instructions are changed. The hardware malfunction causes in its turn a software malfunction that may not be discovered for a while (Lane,1985). Banks unfortunately do not automatically accept the liability for problems arising from faulty equipment .

Finally, certain safeguards are built in to the hardware for security purposes. Mechanisms can be set up to protect the data and programs held in main memory. Whether memory protection is achieved through the use of bounds registers, locks and keys or access control bits, faulty equipment may allow the control to be by-passed, enabling the contents of main memory to be accessed. This is particularly serious if PINs or encryption keys can be discovered.

5.4 Error

Inadequate precautions may be taken to guard against the other threats described. It is impossible to list all possible failings but some of the most important are given below:

- no arrangements made for a back-up computer and site in case of disaster
- failure to draw up and test a contingency plan so that a disaster leaves the organisation vulnerable
- the computer centre is located in a high risk environment, below flood level or near an oil plant, for instance

- poor administrative procedures to prevent fire, with no control of the storage of flammable materials
- no heat or smoke detectors or inadequate fire fighting equipment
- no back-up power, operations are held up by a power cut
- poor maintenance of hardware with the consequent malfunctioning of equipment
- inadequate staff training, the computer may be accidentally brought down by the operator
- predictably scheduled periods of computer down-time that help a criminal to plan a crime
- hardware damaged accidentally as a consequence of staff carelessness : a disk may be dropped whilst being moved; food or drink may be spilled over the computer causing it to malfunction.
- lack of physical security, the computer centre is open to both staff of the organisation and outsiders, making attacks from inside and outside the bank possible.

5.5 Computer abuse

5.5.1 Interference with hardware

There are various ways that staff can interfere with hardware for their own purposes :

- circuits can be modified to allow security controls to be circumvented. Unauthorised modification of hardware operating system security controls by hardware engineers, for instance, makes the system vulnerable to attack

- a member of staff may deliberately crash the system. A system is often vulnerable after a failure has brought processing to a stop. On re-start a program runs in supervisor mode and this allows the user to access all the privileged operating system instructions that can be used to help carry out and cover up a crime (Krauss and MacGahan,1979)

- hardware may be replaced without permission. In one case a diskette was substituted causing an AS$20,000 loss (Mason,1985)

- the central processing unit can be interfered with by activating interrupts from the computer console. In a German bank fraud, the operators prevented bookkeeping entries by activating system interrupts. As a result, invoices were prepared without the transactions being recorded on file. The operators received payment for these (Hayward and Kemp,1987)

5.5.2 Theft of equipment

Any moveable equipment can be stolen from the computer room. Tapes and disks can be stolen either for their value as hardware or for their contents, data or software. In a variation on this theme a maintenance engineer might inform the computer operations manager, quite untruthfully, that a disk is faulty. He could then replace it, taking away a disk full of information.

5.5.3 Extortion

An individual or criminal gang might use the threat of internal or external attack to extort money from an organisation. Threats could be made to bomb the computer suite, for example. The removal of tapes and disks together with their back-ups can also be sufficient to stop the bank functioning, with a large sum of money asked for their return. Although the theft of storage media is involved, this is essentially an attack against an organisation's data and is dealt with in section 7.5.10.

5.5.4 Misuse of computer resources

Unauthorised use of computer time is a risk that has to be considered. As Bequai (1983) notes computer time is a valuable commodity; its unauthorised use whether for playing games or running a business can cost a bank money. Two programmers employed by Sperry Univac used the company's computer to run a music arranging business. They

developed a program to turn out sophisticated musical arrangements as well as maintaining a record of their business transactions on the computer. They were charged with misusing US$144,000 worth of computer time (Norman,1983).

5.5.5 Vandalism

The computer installation can be wilfully damaged without the intention, however, of halting operations. The following example which is not from the banking industry illustrates the risk. Burglars who discovered that there was only $150 in an office safe used the welding equipment on office equipment and furniture. In the resulting fire the building was gutted and the computer room next door was damaged by smoke and soot deposits. As a result the whole computer system had to be written off (Wong,1987).

5.5.6 Misusing computer maintenance

For the purposes of routine maintenance, the computer may be shut down for a short period. During this time, it is possible to exploit system weaknesses that may have been overlooked. A fraud ring was able to steal approximately US$100,000 from a bank that failed to verify PIN numbers in ATM transactions during nightly maintenance periods. Stolen cards were used to make the withdrawals during the scheduled periods of computer down-time (Bank Fraud,1987g).

5.6 Sabotage

The computer can easily be damaged, computers have been set on fire, shot at and bombed. Internal attacks on the installation and its associated components might be made by disgruntled or mentally ill employees. Sabotage from outside the organisation can be the work of terrorists, competitors or anyone sufficiently aggrieved to launch an attack on the computer installation. Recent incidents indicate that terrorists perceive computers as a symbol of capitalist society and seek to harm economies through attacks at one of its most vulnerable points. There is also the chance that a competitor will seek to harm an

organisation in this way. Bequai (1983) cites a case where the computer was sabotaged to prevent it functioning as a viable business entity; the publicly traded stock fell in price as word reached Wall Street that the company was in financial trouble. Events of the following type may occur :

- organized raid by outsiders followed by systematic destruction of equipment
- unlawful occupation of the site
- radio-frequency interference
- planting of explosives.

Sabotage may also be carried out on a smaller scale by members of staff; systems programmers, operations managers, and console operators all have the opportunities to damage terminals, disk drives and consoles. Media librarians and job-set up clerks can destroy the storage media such as disk and tape in order to corrupt the data and software. The apparently accidental spillage of orange juice over a disk can be sabotage. The list of possible acts is limited only by human ingenuity and even quite trivial acts can have serious consequences; the setting on a disk can be altered bringing the system to a halt, the Central Processing Unit can be interfered with to disable security controls and so on.

Examples

1.The head of Scotland Yard's computer crime unit told a conference that electronic funds transfer was a prime target for terrorists since it was the best potential source of money for terrorists. He pointed out that whilst electronic funds transfer accounted for only 2% of transactions, it represented 83% of their value. Terrorists had also realized, he continued, that electronic funds transfer systems were the easiest point at which to disrupt economic life The Red Army Faction in West Germany narrowly failed in its attempt to bomb a bank. If successful they could have halted all financial activity in West Germany for 3 days (Black,1986).

2. An operator employed by the National Farmers Union Corporation short circuited the internal disk drive by jamming a metallic object between the circuits. Over two year period this was repeated 56 times. The trouble was first attributed to power fluctuations and new wiring was installed. Further precautions included back-up disk drives. Approximately US$500,000 was spent trying to track the problem down. The culprit was only caught after closed circuit TV was used to monitor the area (Hayward and Kemp,1987).

5.7 Conclusion

Certain important issues arise from the identification of the risks to hardware. Since systems are so vulnerable to disaster or sabotage, attention should be paid to the location and design of the site with back-up facilities provided for emergencies. When choosing a suitable location, topographical features such as weather conditions, proximity to a river or earthquake fault should be investigated. Even if no real choice of site can be made, then at least the bank should have some idea of the likelihood and possible costs of a disaster.

Examination of banks in the United States by Federal banking agencies often result in recommendations for back-up computer centres (Seif,1984). The four alternatives described are in-house, service bureau, reciprocal agreement or recovery operation centres (ROCs). The in-house solution can involve completely duplexing operations but, in view of the costs incurred, it is more probable that a bank will transfer processing to another of its sites. Service bureau and reciprocal agreement are unlikely to be satisfactory considering the communications requirement with on-line systems. A recovery operation centre may be either a "hot" or "cold" site. With a "hot" site, the appropriate hardware and communications equipment is already installed whereas a "cold" site has only the required services, power and air conditioning etcetera, but no computer. Whichever alternative is selected, a disaster recovery plan should be drawn up and tests should be made at regular intervals to check that the change-over from one system to another goes

smoothly. Some degradation of service is almost bound to occur. Any security risks associated with the restricted service, for example, off-line ATMs, needs to be carefully evaluated.

The physical security of the computer room and hardware is also a matter of some concern. The site should be protected and access to the computer centre restricted to authorised staff only. Personnel must be carefully vetted particularly in view of the fact that low paid employees such as operators are in charge of very expensive equipment. Finally, the organisation should carefully supervise the activities of staff so that they have no opportunity to make serious mistakes or put malicious schemes into practice.

Chapter 6

Threats to software

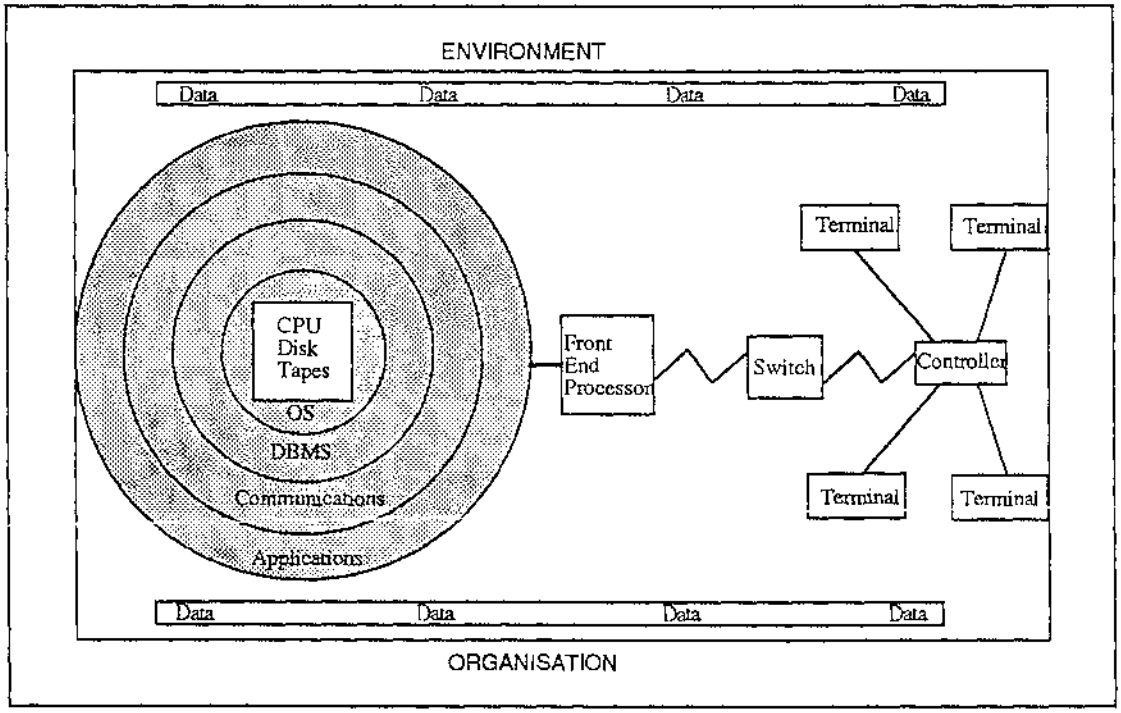


Figure 6.1 Software

6.1 Introduction

In this chapter the threats to software are identified under the headings disaster, accident, error, computer abuse and sabotage. The purchase and development of software represents an enormous investment for a bank. The various types of software required have already been discussed in section 3.5. These programs are particularly at risk from error, unauthorised modification or destruction. Since the integrity of the data and the on-going operations of a bank depends upon software, the exposure of a financial institution is very great when appropriate protection is not provided.

6.2 Disaster

Since programs are stored on media such as tape or disk, they can be destroyed as the result of a fire or other disaster. Hard copies of software and associated program documentation may also be lost. Precautions such as the off-site back-up of software and/or storage in fire-proof safes are often taken to ensure that an organisation can keep functioning after a disaster. Even this is not sufficient if the disaster is so great that the off-site software is also affected or if careless back-up procedures mean that up to date copies of vital programs are not available.

6.3 Accident

A minor disaster can affect software. This can take the form of a disk-head crash or damage to a terminal. All that should result is a temporary hold-up in processing whilst a back-up copy is loaded and tested. (It is assumed that the latest version of a program is readily accessible. Of course, if this is not the case, the hold-up may last longer).

6.4 Error

6.4.1 Errors in the software lifecycle

The development of application software follows a well-known cycle : system specification, coding, testing and maintenance. Software that has not been designed to cover all contingencies or has coding errors due to insufficient testing can have catastrophic consequences. Current system development is an art rather than a science. Whilst terms such as software and information engineering are widely used, the tools available do not give the mathematical precision traditionally associated with engineering. Formal specifications and proofs of correctness are developments that should perhaps be monitored closely by the banking industry. Development methods such as HOS, widely used by the United States Department of Defence may be relevant in an environment where error is costly (Martin,1983). Without such tools it is possible for errors to occur at one or more of the following phases :

6.4.1.1 System specification

At this stage the system should be specified unambiguously so that all the needs of the user are met. Unfortunately, when the software is designed flaws often creep in that may or may not be found before the software goes into production. Sometimes systems analysts fail to anticipate the actions of others and leave the way open to ingenious criminals. Finally, an audit trail and control totals may not be included. Weak points in software can be exploited by criminals. Davies and Price (1984) observed that the design of electronic banking systems requires much more attention to data security than was the case in the past. The security precautions taken can be studied by criminals over a long period, if the potential gains are large enough, before they devise an elaborate attack. Since the systems are automated, a successful fraud may be repeated several times before discovery.

6.4.1.2 Coding

The written system may not accurately implement the specification. A publication by Members of the British Computer Society Working Group on Testing (1986) reported that in one study very experienced programmers were found to make one error in every 30 lines of code, with inexperienced programmers performing far less well. Pressures of time and inadequate supervision of staff both contribute to this state of affairs. The problem is compounded by the fact that, as there are so many pathways through complex programs, it is impossible to prove that a suite of programs will correctly process data.

6.4.1.3 Testing

Ideally, testing takes place at all stages from the design specifications through to programs and the completed system. Errors often remain undiscovered during the testing phase because programmers consistently underestimate the number of tests required to verify a program and fail to pick up errors in a piece of code when desk checking it (British Computer Society Working Group on Testing, 1986).

6.4.1.4 Controls

Controls should be built into the software to validate input (using check digits for instance), to generate control totals and to log all completed or attempted transactions (this often referred to as the audit trail). If these basic controls are omitted then it is impossible to verify whether all transactions have been processed correctly.

6.4.1.5 Maintenance

Proper software documentation might not be kept; when changes have to be made to the program no-one fully understands the impact this will have. Modifications made in these circumstances can have unforeseen consequences - calculations might be incorrect or audit controls by-passed.

Whatever the reason, software that is defective can cause a bank many difficulties. If the application software is faulty or fails, data may be lost, transactions processed twice or totals incorrectly calculated, the records and files on the system will not reflect the transactions that were made. Furthermore, application programs have to run in conjunction with other software, for example database or communication, and insufficient testing of the interface may result in the transmission of inaccurate and unreliable data. It is particularly serious if faulty software brings the whole network down and transactions can no longer be handled. Finally, if the operating system, which is large and complex, is full of flaws, this allows criminals to circumvent controls, access data or erase the audit trail.

Examples

1. Westpac had to close down its Handybank ATM system because of a software error that had not been discovered during testing. Apparently, new software had been installed which inadvertently allowed ATMs to pay out money to customers who did not have sufficient funds in their accounts. Westpac was able to recover these funds from customers since all transactions were recorded but was undoubtedly damaged at the public relations level (Kaye, 1987).

2. A software error cost the Bank of New York more than $US4 million according to a report in the newsletter of United States organisation of Computer Professionals for Social Responsibility. The treasury bond market's delivery and payment system was brought to a halt for more than 24 hours. The bank was not able to deliver securities or make payments to sellers. In order to pay for securities already received US$20000 million had to be borrowed from the Federal Reserve. The interest on this loan was US$4 million.

3.The bank of America acknowledged that conversion to a new trust and accounting system had resulted in a loss of US$23 million. A new system "MasterNet" was brought

on-line before being fully tested. The system crashed for days at a time with the bank months behind in providing customers with monthly statements and costly delays in the trading of securities (Hoffman,1987).

4. The Computer Fraud and Security Bulletin (1985c) reported the case where an American youth discovered that by keying in a certain code his withdrawals from ATMs were not debited to his account. Within a twenty four hour period he and his friends withdrew US$40,000.

5. Joseph Herman transferred money between his accounts by filling in the appropriate forms. Subsequently, when accessing these accounts by ATM card, he found that the money had been transferred from one account but was not available in the other. A printout of the account revealed that the funds were transferred but the author was still not able to access the money by his ATM card. It transpired that when the initial transfer was posted the computer went down. This led the account to be double flagged so that the account balance available by ATM remained the same as it was prior to the transaction. The money was later posted properly to the appropriate account but the double flag was not cleared. Double flags were usually cleared after two days but for some reason unknown to the bank manager some of them did not expire. If the author had not queried this matter, the money would have been in an account earning interest but would have been completely inaccessible (Herman,1987).

6. Many Australian Building societies were affected by a US$31,400 ATM fraud. A teenage boy after making a complex set of transactions including deposits which were immediately cancelled, was able to withdraw considerable sums of money. The fraudulent transactions were made at night when the ATMs were off-line. The transactions were switched from the ATMs through the Ausnet switching network to a switch run by a computer company. Through a unique set of circumstances that the

program had not been set up to handle, it was possible to make the illegal withdrawals (Retail Banker,1985).

6.4.2 Omissions

Appropriate procedures should be in place whilst programs are being written or after they are put into production. Negligent acts such as the following make it easier for errors to creep into programs or for fraud to be committed.

- the wrong program or an out of date version of it is run by the operator
- production, source and load libraries are not kept secure. Software might be lost or taken by someone who changes it or holds the bank to ransom for its return
- the principle of segregation of responsibility is not practised so that responsibilities for writing, modifying and/or running programs are not divided. Too many functions can be placed with one person, giving him the opportunity to make unauthorised changes, run his own version of a program etcetera. It is perhaps worth noting that the whole concept of user computing may be inappropriate in a banking organisation (see section 9.7.7)
- failure to keep a current version of software relevant documentation at the back-up site. If a disaster such as an earthquake does occur and an organisation has to switch processing to its back-up site, there will be problems if the latest version of a program or the required operating details are not available
- systems implemented without sufficient training. Without full training, a new system may have teething problems when the change over occurs, with staff unable to understand or carry out their duties properly
- failure to keep operating manuals up to date. In the case of a hardware disaster when processing is transferred to another site, it may take time to get programs running because the required details are not available

- failure to document software properly. If programmers do not document programs at the time that code is written, it becomes very difficult for those who have to maintain programs to make changes that do not have unforeseen consequences
- operating system controls such as authorisation tables which identify the users who are allowed to access and run programs should be put in place. If programmers are allowed to run the software, thus violating the principle of segregation of responsibilities, they have the opportunity to run unauthorised versions of programs
- inadequate change controls. If the bank does not set up and enforce change procedures then programmers have the opportunity to make unauthorised or erroneous modifications to software. Suitable program change controls should be in place - changes should be approved, tested thoroughly, documented and signed off to show that the program is safe to run
- software still being tested may be allowed access to database records. This not only allows programmers access to possibly sensitive information but can result in the corruption of the stored information as a result of flaws in the program

Example

A programmer who was seen by senior bank management as above suspicion was given special assignments directly, often bypassing his immediate superiors. Over time, his manager became accustomed to the programmer working on special projects and did not question his activities. The perpetrator took advantage of this laxity to make unauthorised modifications to computer programs. At least US$1 million dollars was stolen from the bank by a clever fraud which involved the perpetrator in using the suspense, inter-branch clearing and un-recorded-items accounts. Money from these was paid into several unauthorised accounts set up by the programmer. The fraud was so complex that even

after it had been discovered (purely by chance) it took months to unravel (Bank Fraud, 1987e).

6.5 Computer abuse

In this section the principle threats to software are identified as well as the opportunities offered to various people to alter programs. Both these issues are dealt with in order to identify those weak points in an institution's organisation that permit a software attack.

6.5.1 Unauthorised change to software

Software may be altered either to carry out or cover up a fraud. Such schemes are described below. Methods of attack that make such changes difficult to detect are also dealt with.

6.5.1.1 Program modification to facilitate fraud

Program modification schemes can be carried out not only by programmers employed by the bank but also by anyone who can submit a job to the computer system or who can access the tape and disk library. Software in the host computers, network switches or the retailer's terminals can be altered to destroy, modify or misdirect debit and credit transactions. Unauthorised input can be permitted or the data on the files modified. Typical techniques (Krauss and MacGahan,1979) include :

- programming the computer to accept undocumented types of transaction. In this way extra transactions can be processed
- changing authorisation messages. This can allow a user to make ATM withdrawal when a certain combination is entered even if there is no money in account
- tampering with files. An individual's credit limit might be raised on the customer master file so that bills can be charged up that the account holder has no intention of paying. Alternatively, all outstanding debts can be

written off. Files such as the hot card file can be altered to ensure that stolen cards can continue to be used

- setting up a shadow system . An unauthorised or shadow system system can be set up to change records or files to allow monetary gain
- altering the software in an ATM or EFTPOS terminal. Software resident at the ATM can be altered to increase the maximum number of bills dispensed. In EFTPOS the transaction amount may be altered in favour of the retailer
- siphoning small sums from numerous sources (breakage). Only a few lines of code need to be added to a program to carry this out this scheme. Breakage is employed when a computation is called for. In electronic banking it can be used when interest on savings accounts is being calculated. A small amount might be debited from each account accessed and added to the balance of the criminal's account
- misposting with lapping. When a program has been altered to allow misposting, this allows debits to the perpetrator's account to be applied to the account of someone else or credits the criminal's account with monies due to another. Since complaints can be expected from those whose accounts are incorrect, the perpetrator covers this up by creating another misposting to continue the fraud

6.5.1.2 Program modification to cover up fraud

To perpetrate a fraud successfully, a programmer can make changes in the software to obliterate all trace of a withdrawal :

1. Balance manipulation

   To cover up a crime (the suppression of a debit) a criminal can modify programs so that all totals and balances appear to be correct for the day (Krauss and MacGahan,1979).

2. Fudging control totals

   Control totals will be altered to hide the details of some other program modification scheme Processing will have occurred that is not reflected in control totals (Krauss and MacGahan,1979). In addition, records of fraudulent transactions can be destroyed to make it more difficult to trace a crime.

3. Suppression or alteration of output.

   Wong (1986) noted that in some instances a Trojan Horse program was used to suppress printed warning messages. Illegal code could be activated by special program switches that even rigorous testing may not bring to light.

6.5.1.3 Circumvention of security controls

The operating system is responsible for verifying the identity of employees logging onto the computer (authentication) and controlling access to objects such as files and programs (authorisation). Unfortunately, the password file and authorisation tables set up to determine the identity and access rights of an employee respectively can be be read or altered by anyone who can interfere with the operating system, particularly the systems programmers. If the password of the system manager, who usually has all rights, is discovered, there is no limit to the objects that can be accessed or the functions (read, update, delete, etcetera) that can be carried out. Alternatively, the perpetrator can change his access rights to grant himself full privileges. An log file recording all access requests can be maintained to monitor the activities of staff. Unfortunately, this, too, is vulnerable to a systems programmer.

The communication system is also open to attack. Ritchie (1987) discusses the various ways users can penetrate the network to gain unauthorised access:

- access to the dial-back security software can expose the security system to manipulation or the insertion of code modules that allow security breaches.

- communication software that controls the link with a switch, initializes the line for each session, maintains the encryption keys, generation and verification of message authentication codes, controls the security module, passes transactions on to the required processing software can be tampered with or used by those not entitled to do so.

6.5.1.4 Deliberate error

Staff in the bank, software houses supplying EFTPOS programs or employed by the suppliers of equipment, might be persuaded to make an error that allows an attack on the system (Smart and Evans,1986). The Mafia commissioned a software designer to develop a wire transfer system like SWIFT for the Arab World (Wong,1987). He was asked to provide a trapdoor that allowed the Mafia clandestine access to the system .

6.5.2 Methods of attack

There many different ways in which staff can launch an attack on data via software, some of which are very difficult to detect. It is essential to be aware of each threat so that the degree of the risk can be assessed. Dr. Frederick Cohen (1987) defines these methods as follows :

1. Trapdoor

   In this case an apparently useful program contains a trapdoor that can be used to collect, modify or destroy data. Some code is inserted into the operating system that allows a felon to subsequently by-pass the usual controls. These pieces of code are often referred to as trapdoors. A trapdoor may be introduced by the initial designer of the system, those that maintain it or anyone who is able to access it.

2. Trojan horse

This is a program that performs services beyond those stated in its specification. The perpetrator might insert code in genuine programs that allows access to sensitive information or the ability to alter transactions.

3 Logic bomb

A refinement of the Trojan horse method is to activate unauthorised code. This piece of code embedded in a program causes damage when triggered by some other condition such as a specific time or presence or absence of some data such as a password.

4. Backdoor

This is an entry into the system generally known only to the designer but sometimes found by others.

5. Worm

This program uses unused processors to perform parallel computations. This allows a worm to propagate throughout a network and may cause denial of service.

6. Virus

A virus program "infects" other programs by modifying them to include a version of itself. The virus can act as the carrier of any code that the attacker wishes to use. This may spread through the whole system or network causing changes to data and programs. As a result of a virus the whole computer system may crash. This strategy allows information entering an area to cause damage. Cohen stated that "the potential damage to government, financial, business and academic institutions is extreme". When used in conjunction with a Trojan horse attack,

there could be widespread denial of services and/or unauthorised modification of data.

6.5.3 Copying software

The operating system and utilities can be used to obtain unrecorded facilities. Stand-alone utilities such as the copy function are particularly dangerous since they may run without any access control protection or log file. Using such an instruction anyone could take unauthorised copies of crucial programs. Considering the large sums of money involved in program development, it is always possible that another organisation might short-cut this process by purchasing copied software. Even if the copied software is used only as the basis of a new system, the development time saved may be incalculable. The author does not usually comment on the degree of risk involved but it seems unlikely that reputable institutions such as banks would do this. Nonetheless, it is unwise to assume anything with regard to computer security and software should be given sufficient protection to avoid this threat.

6.5.4 Extortion

Criminals might attempt to extort money from an organisation in various ways. A logic bomb might be planted in the software to be triggered if a suitable payment is not made. Programs can be taken from the library and from a back-up location so that the credit card statement program, for example, could not be run.

6.5.5 Disclosure of software

System programmers may disclose the details of software to those who can then make an attack on the system. For instance details of a trapdoor in the operating system may be made available to criminals, enabling them to circumvent the operating systems access controls.

6.5.6 Running unauthorised software

Unauthorised software (operating systems, application, communications, etcetera) can be run to enable an individual to by-pass security controls, to commit a crime or to cover it up. Master files can be updated by a criminal's own copy of an application, probably a modified test version of a program.

Fraudulent changes made to an application system just before a run and subsequently removed make it very difficult if not impossible to find out how unauthorised modifications occurred. The Computer Fraud and Security Bulletin (1986) published an article which outlined an ingenious method of running one's own version of a program instead of the production copy. The sequence of events is outlined as follows:

- backup programs and data are removed from storage
- unauthorised copies of the program and data are made
- the copies are read on an unprotected machine and fraudulently altered
- the altered files are returned to the backup storage
- a clean copy of the files is retained by the attacker
- the production version of the file concerned is crashed on the machine
- the fraudulent version of the program is loaded and fraud committed
- the fraudulent file is deliberately crashed
- the clean backup copy is loaded.

The item concluded that after the event, such a fraud would be very difficult to detect! In this case an application or systems programmer with knowledge of the area could make

the change. There would need to be some collaboration with an operator, however, to ensure that the fraudulent version of the program is loaded.

6.5.7 Rerunning, restarting or cancelling jobs improperly

Although operators are often low paid they still hold a very responsible job, working as they do in the computer centre. Alagar (1987) considers that they are extremely vulnerable to bribery and could easily act as accomplices, rerunning, restarting and cancelling jobs as required. In electronic banking, it is the batch-oriented credit card and off-line ATM applications that are vulnerable in this way.

6.5.8 Opportunities

There are many different groups with the opportunity to attack the bank's software.

1. Systems programmers

   System programmers who have the responsibility for maintaining the operating system and security software are an extremely able group. Indeed their role is so crucial that Winters (1985) remarked that systems programmers may represent the greatest single security exposure in the entire organisation. They are in a position to patch programs (that is change the executable code), alter the log of accesses to the computer and manipulate the security software to allow unauthorised people to access programs and data files. Particularly in an emergency, for instance to get a real-time program back on-line, it is possible to patch these programs using a utility like SUPERZAP. SUPERZAP inserts bit strings into object code without this being recorded on the log file. Without stringent controls, such activities can easily lead to fraud.

2. Operators

   Operators are in a position to collude with others to run unauthorised versions of software or to help in the commission of a crime by running a program twice or cancelling a job.

3. Systems designer

A systems designer can introduce features that are there solely for his own benefit. Application software can have 'hooks' built into it by the software designer. Once the program has been put into production then these unauthorised modifications will allow fraudulent schemes to be implemented.

4. The programming manager

The programming manager who is in charge of a project can develop a system that meets his own as well as user requirements.

5. Programmer

A programmer on the development team may insert unauthorised code; he runs the risk though that this will be discovered during testing. During the testing phase, tools are available to allow the rapid change of code. They can be used by a programmer to introduce trapdoors into the security-handling and audit control parts of the system. If there are poor change controls in an organisation a programmer can modify code whenever he wants. Even if changes have to be authorised, a programmer just has to wait until an alteration is necessary to take the opportunity to modify the program to suit his own purposes. The opportunity to do this might arise during an emergency. After an unsuccessful run of the program, controls are likely to be at their weakest and unauthorised program changes can be made at this point.

A final comment comes from Jackson (1986), "Systems development people are hired for their skills in analysis, design, building and testing systems, the work involving searching systematically for and remedying flaws and exploiting technological capabilities, a work description that has much in common to that of the process of embezzlement."

6. Any staff member

   It might be possible for anyone to surreptitiously modify a program by removing it from the library unobserved or by convincing the librarian to release it without authorisation. The most dangerous situation might occur in terms of end-user computing where the user defines the problem, builds the system and runs the program. This problem is highlighted in section 9.7.7.

7. Hacker

   Software might be accessed by a hacker. In an interview on American television, a hacker admitted that one of the easiest ways to learn a secret code was to telephone someone in the target organisation and say that he had just started work in the EDP centre and needed to know the password for a particular program. He would explain that at the moment the supervisor was unavailable. Apparently staff were so helpful that this ploy often worked (Saunders,1985).

6.6 Sabotage

Sabotage directed at software can take one of the following forms :

1. Removal or destruction of programs so that the electronic banking applications cannot run.
2. Errors are deliberately introduced into a program so that it fails in certain circumstances (on a particular date, for instance). Again, operations will have to be halted, possibly with serious consequences for the bank.
3. The controls can be altered to allow erroneous data to be accepted. If this occurs the integrity of the database is seriously compromised. A bank would lose considerable customer goodwill if incorrect statements were sent out to customers.
4. Malicious alteration of operating manuals so that programs cannot run.
5. Changes may be made to documents and programs held at the back-up site so that recovery from a disaster is impeded.

6.7 Conclusion

Software faces a multiplicity of risks, the principle of which are the accidental introduction of errors into programs during both the development and maintenance phases and the unauthorised modification of programs. The first threat can be countered to some extent by using a development methodology such as HOS that produces provably correct code although this is no help if the specification is wrong. Thorough testing at every stage of software development is another useful measure. The risk of unauthorised changes being made can be dealt with by incorporating appropriate controls into the design of the system. The EDP auditors should be involved from the earliest stage; establishing effective change procedures and checking that, as far as possible, the program performs its stated function only. Unfortunately, as Clark (1986) stated, " present software engineering tools and/or techniques preclude the development of truly secure software." The fundamental problem as he saw it was that software engineers do not know and/or cannot prove beyond any doubt that the software they construct, integrate and subject to comprehensive testing is penetration proof.

Chapter 7

Threats to Data

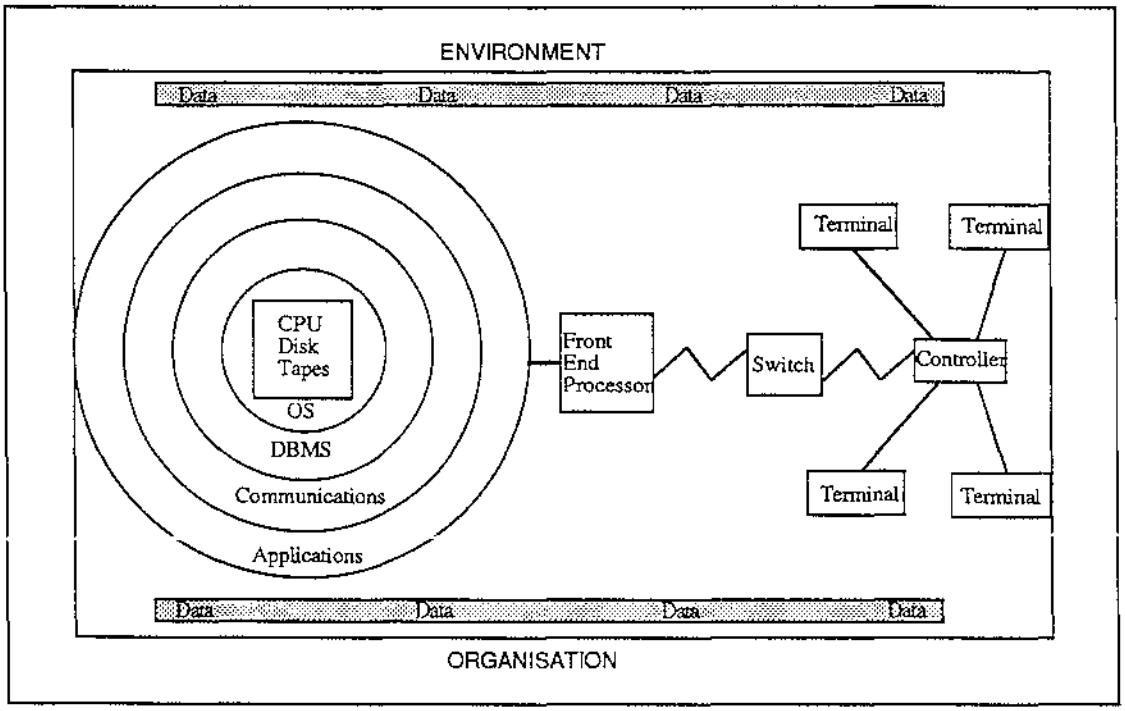


Figure 7.1 Data

7.1 Introduction

In this chapter, the threats to data are identified under the headings of disaster, accident, error, computer abuse and sabotage. Data is an invaluable asset of the institution. It provides the information needed by a bank to function and, in many cases, such as a customer's account balance, directly represents money. Indeed, most of the money handled by a bank is represented by data and not by cash or gold. The different kinds of data in electronic banking systems, identification, customer, control and financial, have already been described (see section 3.3). Data is central to information systems; it is stored on hardware, transmitted along communication lines and processed by application software. When this data is unavailable, for whatever reason (disaster, accident or sabotage) applications cannot run. Errors also have to be guarded against otherwise the stored information is not reliable. Mistakes can result in a financial loss either to a customer or the bank; both of these have undesirable consequences for the financial institution, particularly if adverse publicity results. Finally, data needs to be kept secure so that it is not accessed by unauthorised personnel or altered in some way in order to commit a theft or fraud. All of these threats are examined below.

7.2 Disaster

Data is stored on media such as disks, drums and tapes. During a disaster of the type described in section 5.2, the media may be destroyed with the consequent loss of the data. Without off-site storage of data an organisation cannot re-start operations. This is not possible where the scope of the disaster is so great that the back-up site is also affected or when the back-up procedures are inadequate with the available information out of date. Since many electronic banking applications are on-line, the problem of back-up may be very complex. Duplicate systems act as automatic back-up but may also be at risk during a disaster if located in the same area as the host processor.

7.3 Accident

Data can be lost or corrupted in the following circumstances:

- an accident such as a small fire which destroys storage devices
- hardware malfunction such as a disk head crash
- failure of the network or mainframe
- terminal malfunction
- noise on the communications lines.

In the first three cases the extent of the loss should be limited and can usually be recovered from if back-ups are available. Noise on the line should only require re-transmittal of the data . The ATM malfunction may cause problems for a customer if the account is debited for less than the amount paid out.

7.4 Errors

Errors are a very serious risk to data in computing systems. If the input is incorrect or processed improperly then the data will have no integrity, that is it may be incomplete, inaccurate and unreliable. Output may similarly be incomplete, out of date or incorrect. Mistakes can occur for many reasons - software that is not fully tested, faulty system design, hardware or network failures and the actions or omissions of staff. The consequences can be very serious since, in banking, data actually represents money and losses may accrue to the bank or a customer.

7.4.1. Incorrect input

Errors can easily happen in electronic banking. If the customer information encoded on the card is incorrect, for example, the wrong account could be debited in ATM or EFTPOS systems. Other mistakes can be made by customers, the account number in home banking or the deposit amount in ATM applications, for instance. Retailers can enter the wrong price in credit card and EFTPOS applications. An undetected transmission error due to noise on the line can alter any of the details, account number, amount, transaction amount etcetera. Finally, bank staff may have to enter and/or verify

data. Credit card data such as the customer name, address or amount of purchase may be incorrect. A wire transfer operator can miskey the transaction details. Some of these errors are not the concern of the bank. If a retailer overcharges a customer for goods then this should be settled by the two parties involved. However, erroneous deposits in ATM systems and the transmission of incorrect information in wire transfer systems can have serious consequences.

7.4.1.1 Erroneous ATM deposit

When making a deposit at the ATM, the amount entered at the terminal or written on the envelope may differ from the value of the cash in the envelope. This may be an accident or a deliberate attempt to defraud the system (see section 7.5.3.7) which goes un-noticed either because the cashier is careless or controls fail to pick up the discrepancy. In a case of staff error, a teenage boy placed a Jaffa packet in an ATM terminal and declared a deposit of $1,000,000. This was not a mistake on his part, the error occurred when the amount was credited to his account. The organisation was not aware of the incident until the teenager admitted what he had done to his school teacher (Bell, 1986).

7.4.1.2 Erroneous wire transfer

The situation with wire transfer systems is especially complex. Transactions have to pass through many channels; the user relies heavily on others for the processing of a transaction. This makes such messages vulnerable to errors. This topic is dealt with in detail by reports from the BAI Funds Transfer Task Force (1984) and the Association of Reserve City Bankers (October 1983). The principle problems that arise are:

1. Miskeying a wire transfer

   The miskeying of a wire transfer can involve a heavy loss for a financial institution. Any of the fields may be altered, amount, currency, customer account number or beneficiary account number. An error that is often made is the addition of extra zeros to the amount. As a result of mistakes of this type, a bank may lose

funds directly if it cannot recover the funds paid out in error or find itself liable to pay compensation to the customer whose transfer was not properly executed. At the very worst a court case for damages could ensue.

The transfer of funds to the incorrect account in particular exposes both the sending bank and the true beneficiary to loss of funds. Incorrect instructions can be sent either because they are not recorded accurately on arrival or a mistake is made when they are transmitted. It is relatively easy to transmit erroneous data, information may be misheard in the case of telephone instructions or misread in the case of telecopier transmissions which are not always of a high quality. If the paper jams temporarily in a telex, altered instructions may be transmitted. In addition, operator error can result in the miskeying of data. The problem is compounded by the fact that the desire to standardize customer information has lead to the widespread use of abbreviations, truncations and short names. Furthermore, the speed with which a payment system moves funds, together with the nearly instantaneous notification of payment advices makes it difficult to recover from a mistake. The sending bank can request reversal of the transaction in Fed Wire but the recipient of the funds may not respond to the request. In any payment system legal action may be required to recover misapplied funds.

Each wire transfer network has its own rules for compensation. These apply to the claim that can be made against the sender bank (which made the mistake) and the receiver bank. Generally these cover matters such as the period during which a claim may be submitted, time limits concerning the maximum duration of the claim and a formula for calculating the interest to be paid. Unfortunately if a customer of the receiving bank has the use of funds and not the receiving bank itself, that organisation is under no legal obligation to pay compensation for use of funds. Moreover, the rules only apply to members of the association and not to

non-participating organisations. Finally, it may take days to realize that an error has been made and a bank is liable to pay compensation for that period.

Example

1. A businessman and his wife on holiday in the Orient ran short of money. An instruction was sent to their bank in the Midwest to transfer US$10000 through the wire transfer system. An operator in the bank instructed that US$1 million be transmitted to the account. The bank did not discover the discrepancy until the couple concerned had spent all but US$80,000. The bank had to accept that the terminal operator had made an error that cost it US$910,000. (Krauss and MacGahan,1979)

2. Test code error

Errors made in generating or recording the bank's test code on outgoing transactions will result in the transaction being rejected at the receiving end. Conversely, if an error is made when testing the codes on incoming transactions so that an invalid transaction is accepted then the bank could lose all the money that it paid out.

3. Late payment

An error made whilst recording the due date of a disbursement can lead to late payment and the consequent liability of the sending bank to legal proceedings. Similarly, failure to act on a source document either because it was lost or through an error would have the same results. The sending bank can even be held liable when a transaction arrives after the due date because the initial message was so garbled that it had to be re-transmitted. Indeed transactions will not be processed in a timely manner if staff do not ensure for both outgoing instructions and incoming credits that all processing steps are documented and maintained for the required amount of time. This is important when messages or payment orders are

received too late to process the same day. If banks fail to settle correctly on time then they face legal action from customers. Very complex situations might arise. De Vallee (1987) pointed out that if a bank fails to make a US$1 million dollar payment required for a bid bond then the client loses not only the contract but the money spent trying to obtain it.

7.4.2. Incorrect processing

Application software that has been poorly designed, coded or tested leads eventually to the incorrect or incomplete processing of data. In the worst case, a valid transaction may be rejected with the result that the appropriate action is not taken. Again, payment to the wrong account or failure to process a genuine transaction has the most serious consequences in wire transfer systems. Software errors have also been responsible in ATM systems for withdrawals of thousands of dollars not backed by funds (see section.6.4.1). Since much processing involves calculations, the various totals, customer accounts, internal accounting etcetera may be wrong. There is also the possibility that the wrong version of a program might be run by an operator with the result that transactions are improperly processed. If production (that is real world) data is used by test software, mistakes may also occur.

Double processing may occur because of a fault in the application or network software. Financial records can also be mistakenly updated twice with the same data if the operator runs a process twice. This could happen with the batch processing of ATM transactions that takes place in off-line systems. There is also the possibility that the recovery software which comes into operation after a computer or communications breakdown may mistakenly direct a transaction to be processed for a second time. Whenever a transaction is duplicated either a customer suffers with a double debit to the account or the bank makes a payment twice. Once errors come to light, processing may have to halt for a time to restore the integrity of the database, by reversing transactions and re-running them

correctly. If mistakes are not discovered quickly both customer statements and bank reports will contain incorrect information and the credibility of the bank will suffer.

7.4.3 Incorrect output

Obviously if incorrect processing takes place then any output generated is likely to contain errors. Output can be defined as the response to transaction requests as well as reports based upon stored data. The failure of an ATM or EFTPOS transaction when there is actually money in the account could be humiliating to the customer. In home banking a customer could be presented with the wrong screen, showing details of another customer's accounts or electronic mail. Finally, there may be many listings of importance such as journals of sensitive transactions, unprocessed transactions and so on. If these are inaccurate the appropriate follow up action cannot be taken. A batch of records that is omitted from the listing of unprocessed transactions will not be re-entered. An unusual transaction will not be investigated making it easier for a crime to be committed.

7.4.4 Loss or corruption of data

An operator is in a position to do a great deal of damage if suitable controls are not enforced : files of data may be accidently erased, the wrong disk mounted or storage media, tape or disk, mislaid. Finally, data that is being processed when the computer goes down may be irretrievable if there has been a failure to record all attempted transactions. Loss of data on a large scale is a very serious matter. It brings into question the reliability of customer account information. Processing might be held up in order to rectify the situation. Disruption of service is a serious matter when banks are heavily involved in on-line services.

7.4.5 Omissions

If standard operating procedures are not followed the quality of the data can be affected :

- inadequate back-up procedures : data may not be backed up regularly or the back-up may not be verified. This can result in corrupt data being stored

on the back-up tapes. This makes recovery, if the need arises, very difficult

- poor access controls allow unauthorised personnel such as hackers to browse through and even change data
- inadequate error handling procedures mean that adjustments to incorrect transactions may be processed after a long delay or may not be made at all. Customer goodwill is easily lost when mistakes are not dealt with promptly
- test software can access production data. This can introduce errors into the database and may also allow programmers to obtain sensitive information
- the principle of the segregation (that is dividing up tasks between two or more members of staff to make a crime more difficult to commit) is not followed making it easier for employees to carry out a fraud
- unavailability of the database. Customer records have to be accessed in order to process transactions. Dick May of the Relay Network, North California mentioned cases where ATM transactions had not been processed because the card database files of the participant institutions were unavailable (Zimmer,1987)
- if audit controls, such as batch validation totals in off-line ATM systems, are not in place or are ignored there is no check that all the transactions have been correctly entered
- failure to balance the system at the end of the day
- failure to check exception reports showing the details of unusual transactions
- output not kept in secure locations so that it can be be stolen or the information disclosed to unauthorised parties
- files are incorrectly labelled or stored so that they are difficult to find when they are required
- tape and disk library not properly maintained, or left unlocked when the librarian is not there

- the financial records may be inaccurate if credits or outgoing instructions are not entered into the internal accounting system
- failure to ensure that the internal accounting system is in balance with the transfer system

7.4.5.1 Negligence by staff at the sender bank

Procedures that have been instituted to prevent fraud might not always be followed by staff. For example, there may be a failure to authenticate the identity and authority of the sender. A bank telephone operator told a customer that the accounts the customer was trying to debit for a transfer were non-existent. Eventually, the customer guessed an authorised account number (BAI Funds Transfer Task Force, 1984). Other possible staff errors include a failure to verify a transfer by telephone call back, completing a transfer prior to checking by another officer in the wire room, releasing the instruction to the wrong transfer system, compromising passwords through a failure to check them regularly, and ignoring or improperly reviewing exception reports.

Sender risk can occur in wire transfer systems as a result of an error when a sending bank pays out funds at the request of a customer who cannot cover the transaction because the funds on deposit are insufficient or uncollected. Alternatively the money in the account is not put on hold when the wire transfer is approved and a customer withdraws the money required to pay the transfer. Obviously, the bank stands to lose funds in this situation.

7.4.5.2 Negligence by staff at the receiving bank

The receiving bank can make mistakes on the receipt of a funds transfer message, even failing to verify the transfer system's identity. When the message is genuine, it is possible to lose the incoming transaction, erroneously reject it or fail to make the appropriate payment. An erroneous transaction may be accepted by a staff member who does not check the accuracy and completeness of the message; a garbled, incomplete or duplicate transfer may be acted upon. More seriously the validity of the incoming credit

may not be checked. A bank employee failed to verify an incoming telex which was later discovered to be fraudulent (BAI Funds Transfer Task Force, 1984). Other poor operating procedures which make an organisation liable to fraud include accepting an alteration to an incoming credit, or allowing deviations from procedures or agreements without the approval of a senior bank officer.

Receiver risk arises when the party sending the funds does not settle. Many banks credit funds sent via CHIPs and other non Fed Wire institutions even if they do not represent collected funds at that time. This processing of a transaction prior to the clearing of funds is most unwise since the sender might not be able to settle. Bilateral arrangements are often arranged which limit the amount that the due from account can reach before the receiving bank will stop accepting credits from the sender. If there is a failure to check this account by the appropriate staff member then the bank concerned might not be able to honour its commitments (BAI Funds Transfer Task Force, 1984).

7.4.5.3 Phantom transactions

Banks usually assume that the data held on a computer system is complete, accurate and reliable. A report by the National Consumer Council in the United Kingdom called "Losing at Cards" pointed out that there are many unrecognized problems in the area of data integrity. It described the many events that could lead to a loss of data integrity (Dominion,1986b).

- double entries made manually after the failure of an ATM
- card and PIN sent to wrong addresses
- interception of the PIN at customers' addresses
- incorrect account number allocated to a card
- malfunction causing ATMs to debit accounts without delivery of money to a customer
- production of money by an ATM after an initial failure to complete the transaction

- the occurrence of phantom transactions i.e. transactions where customers deny being responsible for cash withdrawals.

In many countries (for instance, England, Australia, New Zealand) concern has been expressed that some ATM withdrawals were never actually made by the account holder. After Channel 4's Network 7 programme dealt with this issue in the United Kingdom, they received over 100 letters from people claiming to be victims of phantom withdrawals (Nutley, 1987). An Australian Consumers Association report dealing with problems in the area of electronic funds transfer published several letters describing the fraudulent withdrawal of funds due to malfunctioning ATMs (Dominion, 1986e). Wong (1986) relates that in one case a withdrawal from an ATM occurred when the customer was on vacation and could not possibly have withdrawn money from the cash dispenser in question.

Banks often deny that errors can be occur. A Barclays fraud investigator told a customer that in the "vast majority of these cases someone in the family turns out to be guilty and that in the very few cases where it could not actually be proved, it was assumed to be the case" (Pehrson,1986a). Analysis of so called phantom transactions in Britain (Wong,86) showed that the unauthorised withdrawals were all made at teller machines in the vicinity of the victims' homes. This suggested that friends or family were making use of these cards illegally, having already found out the PIN. For example, it is possible to obtain a PIN by watching the cardholder enter it. Later the card may be stolen, a withdrawal made and the card replaced. The BNZ in New Zealand has recently included a warning that appears on the display screen advising customers to make sure that no one else can see the PIN being entered. There are many other reasons though why an error might be made - internal fraud, malfunctioning equipment or an error in the software.

Even if the amounts concerned are small, and this is not necessarily the case,the problem is not trivial. If a genuine customer complaint is ignored then there is a loss of goodwill.

Possibly the bank's reputation in a certain locality can be affected. On the other hand if false claims are accepted then the bank has laid itself open to fraud.

Examples

1. A New Zealander lost a Post Office bank card which could also be used to make withdrawals from an ATM. The loss was reported on discovery and there was no PIN, it was claimed, with the card. $300(NZ) was subsequently withdrawn from various ATM locations. Eventually the Post Office accepted liability. (Dominion, 1986c).

2. In one case quoted by the Dominion , Des O'Dea of Wellington described his attempt to withdraw $50 from an ATM. No cash was dispensed but the transaction subsequently appeared on his statement. After querying this, the bank found the transaction details were so garbled that they reversed the transaction (Dominion, 1986d).

3. Alex Heatley obtained only $80 when requesting $90. After he reported the error, he was informed that he would have to wait until the machine was balanced before his claim could be dealt with. The machine did contain $10 more than it should have done and so this amount was paid over to him. He was particularly concerned, however, that if the machine had incorrectly dispensed money to others then he would have been suspected of fraud. (Dominion, 1986d). This was not an unrealistic fear since Broadbank in New Zealand have been quoted as saying "The most common but still extremely rare problem is under or overdispensing of notes since this relies on a mechanical note picker". (Pehrson, 1986b).

7.5 Computer abuse

The unauthorised use of passwords, masquerading as a legitimate customer, data manipulation and taking advantage of a genuine error are the main exposures a bank must guard against.

7.5.1 Unauthorised use of passwords

A password is not only a method of proving the identity of the computer user; it may also define the users rights on the system, the programs that he can run and the files that he can access. Unfortunately, passwords are a notoriously poor means of authenticating the identity of a database user (EDPACS,1985b), (Kemp, 1985). The principle methods of breaking password security are well known and are only discussed briefly below.

1. Employee negligence

   Since passwords can be difficult to remember, authorised users write them down (on a terminal or in user manuals) or chose passwords that are easy to guess such as their first name. Even when members of staff are required to change their password at regular intervals, old favourites are often re-selected. Passwords can also be discovered by someone who observes the password entry process at a terminal. Finally, when an employee leaves, there may be no procedure for removing the password from the files. The ex-employee can still access the database.

2. Linetap

   The signals transmitted from the terminal to the host computer can be recorded on to tape via a radio transmitter and re-played to a compatible terminal. In this way, the plaintext passwords of some users can be obtained.

3. Trojan Horse

It is possible for an authorised user to include unauthorised code in a program allowing him to access the contents of the password file. If this information is not encrypted then all the clear text passwords on the system are available including those that have full privileges, such as the system manager's.

4. Operating system weakness

Many operating systems provide the opportunity to access the password file. In EDPACS (1985b) full instructions for accessing the PASSWORD file in MVS, the IBM operating system often used in banking, are given .

5. Terminal simulation program

A program can be written to generate the log-on screen that a genuine user expects to see when signing on to the computer. The employee enters the user code and password which are recorded in the criminal's file. The logon procedure then appears to fail so the user tries again, this time he is connected to the real operating system. A terminal simulation program was discovered at a major credit card company where the program was used to capture passwords to an important on-line customer accounting system (EDPACS, 1985b).

7.5.2 Masquerading as a legitimate customer

The identification and authentication of the customer carrying out a transaction in electronic banking is of vital importance if others are not to gain unauthorised access to funds. Since there are various ways of establishing the credentials of the customer depending on the application, card, PIN, user identification and passwords, there are many different ways of circumventing the controls in place. These will be described in some detail for each method of identification and authentication.

7.5.2.1 Cards

Plastic cards are usually issued in credit, ATM and EFTPOS services. Credit cards are more vulnerable than cards used in the other two electronic banking applications as the customer is not generally required to provide a PIN; unsecured credit is made available to those who present the card at a merchant's and whose signature corresponds with that on the card. Certain checks can be made such as obtaining the approval of the card issuing institution when a transaction is above a pre-set limit or looking up the account number in a file of lost or stolen cards but these are limited in their usefulness. In ATM and EFTPOS services on the other hand it is not sufficient for the customer to be in possession of a card; knowledge of the PIN is also needed for a transaction to proceed. This card and PIN combination does not eliminate all danger, however. It can be surprisingly easy to find out the PIN associated with a card (see section 7.5.2.2). The principle threats associated with the use of plastic cards are outlined below, mentioning where necessary the service being used. It should be noted that in some cases, a bank issues a card that can be used for credit, ATM and EFTPOS purposes.

7.5.2.1.1 Counterfeit cards

Cards of every type can be counterfeited.

1. Credit cards that make no use of the magnetic stripe

   Organized crime in the United States of America and Asia is heavily involved in credit card fraud. Blank cards can either be stolen or illegally printed by silk screen and offset printing methods (Kelleher,1985). Details of genuine accounts for embossing on the cards can be obtained from shop employees who have access to the transaction dockets. Carbon copies discarded by customers are another useful source of information. Internationally, during 1983/1984, Visa and Mastercard together lost US$36 million as a result of fraud of this type (Burford,1986). This crime is difficult for a retailer to detect since the customer signature will match that on the counterfeit card.

In order to avoid the possibility of a counterfeit card fraud, plastic cards with secure properties are currently on the market. In addition to the stripes, the card may contain a radioactive bar or an embossed hologram for example. There is some dispute about how secure such cards really are. An expert in holographic reproduction systems copied the embossed hologram from a plastic card. (Retail Banker, 1984). Mastercard replied by stating that the copying process was not a security threat since the copy had less depth than the original and the difference would be detected on a plastic card. The process, it was decided, was suitable only for one-off copies but not for continuous copying. This answer does not really address the issue since embossed holograms can already be copied onto holographic film and the technology may improve to make large scale copying of the hologram possible. Since the cards are only examined superficially, a shop assistant may not have the time or competence to detect a fake.

2. ATM, EFTPOS and credit cards that make use of magnetic stripe card technology. It is not difficult to duplicate the magnetic stripe on cards. The end result depends on both the method and the degree of skill of the forger; a copy may be so good that it is virtually indistinguishable from the original or so poor that it is not accepted by terminals. The most commonly used methods are referred to as skimming and buffer recording (Lipis,1985). Skimming involves transferring data from one magnetic stripe to another with no mechanical motion. Heat is applied to a piece of recording tape placed over the stripe of a good card, even a household iron would provide enough heat. The tape produced is laid over the appropriate stripe on a blank card and the heat re-applied. In this way several duplicates can be prepared. A better quality card, however, is produced by the more expensive and complex technique of buffer recording. An electromagnetic card reader has to be acquired or built and used to read the information from the card. This data will then be written out on a blank card that may have been stolen from the manufacturer's stock or illegally printed. Finally, cards can be

manufactured using account details taken from receipts left in the vicinity of the ATM or obtained by wiretapping the communication lines.

A magnetic stripe card can be duplicated very cheaply. A competition held in America to find the fastest card duplicator was won by a student who reproduced a card in less than an hour at a cost of a few dollars (Louis-Noel Joly, 1985).

3. Magnetic stripe technology plus secure properties

A security feature can be included in the magnetic stripe. The EMI watermark stores a number on a card which is related to other data so that it cannot be altered or forged. If a card is counterfeited, using blanks with a watermark, the system will not accept it since the number will not be the one required by the checking algorithm. This is not proof against criminals. Russell Hogg (Brown,1986) of MasterCard stated that "Even some security features such as the encoded magnetic stripe can be duplicated inexpensively by those with a working knowledge of electronics" Although Mastercard introduced measures to combat counterfeiting, it still lost US$17.5 million in 1984. In Germany some cards carry a modulated mark (MM) printed invisibly on the front and read by special sensors in the ATMs. Again, this number is mathematically related to the data on the card. Apparently this mark can also be revealed by certain optical filters under infra-red light. It is possible for a forger to cut up old cards to obtain matching MM numbers for the new card. Experiments by officials at a bank in south Germany showed that this could be done (Catterall, 1986).

4. EFTPOS and credit cards that incorporate the microelectronic chip.

It is the opinion of Mike Lacey (Bemrose security printing) that "the technology used in chip cards is more difficult to counterfeit than magnetic stripe cards, but not impossible" (Brown,1986). Russell Thomas (1986), research project manager with Databank in New Zealand, though, claimed that it would be

prohibitively expensive to manufacture counterfeit smart cards. Since widespread publicity has been given smart card technology and with sales predictions in the hundreds of millions, the time and money that needs to be invested by criminals to successfully counterfeit such cards may well be forthcoming.

Example

1. A major credit card company lost more than US$2 million as a result of a counterfeit card operation. The criminals concerned obtained a copy of the computerized customer master file. A large number of counterfeit cards were produced and the valid names and account numbers were printed on them. Once the accomplices had signed the cards, it was easy to make fraudulent purchases. The signatures were satisfactory and the cards appeared valid so no suspicion was aroused (Krauss and MacGahan,1979).

7.5.2.1.2 Fraudulent application for a card

In this case the applicant for a card provides incorrect information together with stolen or forged identification. The credentials of a potential customer are usually carefully examined to avoid losses through fraud and bad debt; a card is only issued after an individual's credit rating has been determined. This stage may involve checking with a credit agency that a customer is a good risk. If this check proves satisfactory then an appropriate credit limit is granted. Often though individuals will flood credit approval departments with false information hoping that one out of ten or twenty applications will be successful. Once a card has been issued, charges are run up without payment being made. Robert Hoxie was charged with theft of when it was alleged that he obtained the credit histories of 38 Houston residents by tapping into a computer system at a local credit bureau. He made use of this information to obtain bank credit cards in their names. He was able to withdraw US$100,000 from ATMs in this way before he was caught. It was also claimed that he wore a wig and sunglasses to avoid detection by the cameras used to photograph those customers making cash withdrawals (Computer Fraud and Security Bulletin, 1985b).

Example

1. An engineer from New Jersey, using 300 aliases, obtained 1000 credit and charge cards. He was able to do this by feeding false data into data banks via a fictitious company that he had set up. He made sure that each alias had a spotless credit record. He had obtained US$660,000 by the time he was caught (Norman,1983).

7.5.2.1.3 Obtaining an unsigned card

Cards are vulnerable during the manufacturing process and delivery. Those who have the opportunity to steal new or replacement cards include employees of the postal service, the card manufacturer or the issuing bank. People living at the same address as the cardholder or even a stranger may also be able to intercept a mailed card. Sometimes cards are automatically sent out to customers after their previous card has expired without checking that the customer is still alive or that the address is correct. Credit cards are particularly at risk before they have been signed. At this stage there is no need to forge a signature when making a purchase. Criminals may have several weeks to make use of such cards before the unfortunate cardholder is billed for transactions not made by him. Similarly, if the card and PIN can both be obtained before delivery to the customer, the criminal has a reasonable period of time in which to make cash withdrawals and EFTPOS transactions. He is only limited by the amount of money in the genuine cardholder's account.

7.5.2.1.4 Use of lost or stolen cards

Fraud involving lost or stolen credit cards is a common offence; all it requires is the ability to forge a signature. Criminals have even been known to ask genuine customers to sell them their card. The customer then reports the card lost or stolen (Burford,1986). Weston (1987) describes how criminals commonly make use of such cards. In the first instance large value purchases that can be quickly resold are made. Later lower-valued purchases that do not require validation are made. It is often the case that a customer does not realize his card is missing until the monthly statement is delivered. In the United

Kingdom the loss in this type of fraud exceeded US$12 million in 1985 (Burford,1986). ATM and EFTPOS cards, too, are frequently lost or stolen. Although a PIN is needed to make use of these, this information is often available to offenders (see section 7.5.2.2). In Australia for the 12 months ended June 30, 1985, 688 ATM cards were taken during a burglary, 653 were removed from motor vehicles, 611 were obtained from attacks on people and 1439 were reported as lost (Burford, 1986). Cards can also be shown to a retailer for cheque guarantee purposes in the case where both the cheque book and card have been stolen.

7.5.2.1.5 Alteration of cards

The details on a stolen or counterfeit card can be changed and the picture in a photo identification card can be substituted. An effective way of altering the embossing on a card is to shave off characters with a sharp knife and then glue them back on to spell out a different name, address, account number and expiration date (Norman,1983). Such action circumvents any check made by the retailer against the "hot" file of account numbers. Even smart cards can be altered, heat can be deliberately applied to a card so that the characters deboss and new ones can be applied.

7.5.2.1.6 Fraudulent charges by merchants

Dishonest merchants and their employees use misplaced or stolen credit cards to create sales drafts for non-existent purchases. Eventually they receive payments for these fictitious sales. Merchants may also collude with others in order to defraud the card issuer. Weston (1987) details several ways in which this can be done. White card fraud is particularly lucrative; it involves the acceptance by retailers of blank cards, produced by criminals, that have no resemblance to issued cards but carry the details needed to produce authentic vouchers. Frauds of this type could also be carried out if smart card technology was used. A device can be used to imitate the responses of a smart card. If used in a remote terminal it does not even need to physically resemble a smart card. Finally, it is

possible for a merchant to defraud a customer making an EFTPOS purchase by entering two transactions when the customer assumes only one has been made.

7.5.2.1.7 Mail order and telephone fraud

When placing orders over the telephone or through the mail, criminals charge the goods either to a valid account number (but not their own) or a fictitious account. If a genuine number is quoted it may have been obtained in the way outlined in section 7.5.2.1.1 above or by bank staff. In California, a group of criminals had the records of 330 account numbers lifted from carbons of charge slips. They charged 185 merchandise shipments to the credit cards of others (Norman,1983).

Example

1 An employee of a credit card company who had the responsibility of monitoring delinquent credit card accounts made use of her position to access the database of customer accounts. She looked for accounts with a high credit limit but a low current balance. These names and account numbers were handed on to accomplices who used the information to purchase microcomputer hardware (EDPACS,1987).

2. An American, Shanklin, scanned the death columns and then obtained account numbers and credit ratings for Visa and Mastercard via his home computer(Computer Fraud and Security Bulletin,1983a). He then ordered goods including a US$50000 computer and charged them to these accounts.

7.5.2.1.8 Use of returned or captured cards

Returned or captured cards have to be carefully controlled else they can be used by staff members. Cards may be returned to the issuer in various circumstances, when they have been sent to the wrong address, for example, or when they have been re-possessed. Cards can also be withheld by ATMs because they are out of date, overdrawn or recorded as lost. A particular problem occurs in shared ATM systems when a card is used in a

terminal not owned by the customer's bank. There may be no procedure to inform the owner's bank. If there are no suitable controls in place over returned or captured cards, staff may take the cards and use them to make fraudulent purchases or cash withdrawals. In the case of an ATM or EFTPOS card, of course, the employee would also have to know the PIN.

Example

1. A bank which had a very effective procedure for the production, storage and delivery of credit cards had very lax controls over the returned cards. No log was kept of cards returned by post and there was no single location to which cards were automatically sent. Some were delivered to the customer service department where the perpetrator of the crime worked. He selected cards that had been returned because of incorrect mailing addresses and used each one for about three weeks. His activities were brought to the attention of a member of the department responsible for countering fraud. The latter allegedly told the perpetrator that he would keep the matter secret if he was supplied with illegal cards. Eventually, the fraud was discovered when several customers began disputing charges to their account (BankFraud, 1987a).

7.5.2.2 Discovery of PIN

The major safeguard in card based systems is the fact that a transaction has to be authenticated by a PIN. The risks with regard to the unlawful discovery of PINs are twofold. Firstly, a person who obtains both a card and its associated PIN may masquerade as a legitimate user. Secondly, just discovering the relevant customer details and PINs allows determined criminals to perpetrate a counterfeit card fraud. If thousands of counterfeit cards were distributed this would be a very serious threat. Such a crime might not be detected until the legitimate cardholders examined their statements or received notification that the account was overdrawn; the cost of this to a bank might be considerable. In the first place restitution would have to be made to defrauded cardholders if the bank wanted to retain their customers. Deciding which transactions

were legal and which ones were fraudulent would be extremely difficult since customer declarations would have to be relied upon. In such circumstances, many people may make fraudulent claims on a bank either accidentally or deliberately. An important side effect of such a large scale counterfeit card fraud would be loss of consumer confidence in ATM and EFTPOS applications.

To prevent such crimes the customer card and its associated PIN information should never be available together. There are six possible ways in which a PIN can be discovered for fraudulent use. This can be done via the card issuing institution, the PIN delivery system, the customers, the communication system, improper operating procedures and the use of inadequate algorithms. All of these methods are considered in some detail in Appendix 1.

Examples

1. Bankers in the United States of America believe that some customers give their PIN and card to someone else and subsequently insist that the transaction was unauthorised. In the United States of America the institutions must make up this loss even if fraud is suspected (Banking Technology, 1985).

2 One bank failed to make arrangements for cards and PINs returned by the post office as undeliverable. They came back to the bank where a dishonest clerk matched the cards with their associated PINs and proceeded to use them (Brown,1983).

3 A bank believed that at least one employee who had access to customer PIN information was involved in a cleverly conceived fraud. Cards were stolen from the homes of customers who had large balances with the bank. Since only the card was taken and the customer was often away from home, the loss was not discovered at the time. The usage of the cards coincided with the beginning of a new statement cycle. This meant that customers did not realize the card was being used until thirty days later. The losses stopped when the bank tightened up its control of PIN information (Brown, 1983).

4. Raymond Bloquet, a French electronics engineer, copied bank customer cards electronically. He then tricked customers into disclosing their PINs by phoning them up, posing as a member of the bank staff. Informing them first that their PIN was being change, he then asked what number they were using at present. Apparently, this procedure never failed. Bloquet was caught after one of his cards blocked an ATM and he made the mistake of returning to the machine the following evening (Brown,1983).

5. A particularly daring crime occurred in Germany. A unit was attached to certain terminals which captured customer cards on the pretext of some error in the transaction. It also allowed the criminals to ascertain which keys on the numeric keyboard had been depressed for PIN entry although the order was not known. In the worst case there were only 36 combinations of the four digits to try before discovering the PIN. The card was not captured after three mistakes as is the normal practice because the criminals set the error counter on the magnetic stripe back to zero after a wrong try. In this way DM80,000 was taken from cash dispensers in Cologne and the Ruhr area (Banking Technology, 1986b).

6. A New Yorker discovered customer PINs by the simple expedient of watching people enter them. If the ATM receipt was discarded, he picked it up to find out the associated account numbers. He then used a homemade imprinting machine to impress on blank white plastic cards the relevant customer details taken from the ATM receipts and the bank information. He withdrew US$86,000 before he was apprehended. The cards that he counterfeited had a flaw and the bank reprogrammed their systems to capture them (Pehrson,1987a). This ex-ATM service engineer was caught with nineteen of the forged cards in his pocket.

7. Two computer freaks from Cologne built a piece of equipment which screwed on to the front of an after hours cash dispenser. It contained a radio transmitter and a device to read a card's magnetic strip and the PIN tapped into the machine's keyboard. The data

was transmitted to the criminals' nearby car. Later it was stored in their personal computer and then transferred as required to a plastic card. In the course of a few months they took about $40,000 (New Zealand Sunday Times, 1986).

8. Galloway wrote about the experiences he had after requesting a bank card. After its arrival he was unable to make use of it since the PIN that he had requested on the application form was not accepted by the teller machine. When he went into the bank to complain, he found after enquiries to head office that he had been assigned another PIN. The teller in the bank read off the card number to an employee in the central office who supplied the correct PIN number. This was written down on a deposit slip and handed to the customer. The procedures in this case were very weak since at least two staff members would know the correct PIN for that particular customer's card. Unfortunately, this did not solve the problems of this customer who a couple of months later again found that his PIN was unacceptable to the ATM. On enquiring once again, he discovered that his PIN had ben changed to that originally requested. The way that this bank handled PINs does not inspire a lot of confidence that PINs are kept completely secret (Galloway,1987).

7.5.2.3 Home banking

There may be several layers of protection in home banking systems. In the first instance a videotex identification and password have to be supplied. When the videotex identification code is, at most, 9 digits long and the password is 4 characters in length then someone can find out this information using a teleprogram within a reasonably short space of time. Maurer (1985) pointed out that some break-in attempts in an experiment were successful after a few days. To guard against penetration of this type other controls, account number, PIN, Transaction Number, have been built in to ensure that only the customer can access the funds in his account. Webster (1985) discusses the ways in which the customer identification and validation procedure can be circumvented without appropriate controls. The customer account number is the first level of identification and

it can be discovered in several ways : it is already printed on most cheque books, a line used by a customer could be tapped, a micro computer could be programmed to generate random numbers until one was accepted by the system and, if account numbers were issued in sequence by a bank, then knowing one account number, such as 1234567, would mean knowing the others, 1234568 and so on. The next level of security is a Personal Identification Number. The dangers of PINs are discussed in section 7.5.2.2. In addition, a third party (family member, friend, office worker) can look over the shoulder of someone while they were homebanking and see the number entered. Even though it is usual not to display the PIN on the screen, it is still possible to see the keys that have been hit. Moreover, as with customer account numbers, a microcomputer could be used to generate numbers until an acceptable one was found. In order to combat these threats HomeLink, run by the Nottingham Building Society, added further security measures. In particular, the customer is provided, by post, with a batch of twenty transaction numbers. Each of these is an autogenerated random number that is different for each homebanking transaction. The customer enters this as part of the customer identification sequence. Each number is used only once. Whilst this might deter those who tap lines to find out the relevant identification information, members of the family or fellow workers would still be able to ascertain this information. Nor do these precautions take account of the possibility that an one or more employee of the bank may be able to obtain all the relevant identification information as well as the random numbers.

Quantin also pointed out since many terminals used in home banking are in private homes their owners can spend hours trying to undo the terminal, cut across the controls inside, feed in false messages and tamper with the telephone connections (Quantin,1985). If they were able to obtain the videotex identification and password of other users, they may be able to collect a considerable amount of money from their account.

7.5.2.4 Wire transfer abuse

In wire transfer systems, it is vital to authenticate the identity of the person initiating the transaction otherwise it is possible for unauthorised payments to be introduced into the system. A fraud of this type can be perpetrated by someone masquerading as the legitimate customer or by a member of staff authorised to initiate such transactions.

7.5.2.4.1 Fraud by an employee of the customer

However instructions for a wire transfer are issued, banks require some proof of identity, usually knowledge of a secret code but in some cases a signature is sufficient. It is possible for an employee who is empowered to send funds transfer messages to misuse their position of trust and send a false transfer. Alternatively another member of staff might discover a password and issue spurious instructions. This can be done very easily when an organisation releases wire transfers direct from a computer to the bank after the password has been entered. In such cases the onus is on the bank's customer to ensure that passwords are kept secret. No method of authentication is fool proof. With walk-in customers and mail request, the signature is checked to see if the the person initiating the transfer is the person authorised to do so. Forgery of the signature, therefore, is another threat to be avoided. An ingenious criminal may actually add or change the signature on the authentication document lodged with the bank and need not fear that his signature will be queried. In the same way, an agreement for standing or repetitive transfer may be established by an unauthorised representative of the customer. It is possible to circumvent even quite complex procedures. When instructions are given by telephone, each customer has to provide a confidential code for identification purposes which is requested and verified. A follow up call to a specified number may also be made by the officer empowered to release the transfer in order to further check the validity of the instruction. Even this may not suffice since it may be relatively easy in the first instance to find out the password. The second precaution can be circumvented by intercepting the phone call to give the required clearance.

7.5.2.4.2 Fraud by outsiders

There is the possibility that criminals may be able to insert a fraudulent transmission on to the communication network by-passing the authorised channel. Whatever checks are built into the system, a fraudulent wire transfer can be sent by someone who has obtained the requisite information (message format, password) by wire-tapping, by collusion with others (employees of a sending organisation, bank or wire transfer systems), by breaking and entering into customer premises or through weaknesses in the operating procedure. Alternatively criminals might threaten someone who is in a position to send or accept a valid transfer. Attention has also been focused on the possibility that organized crime will pressurize members of staff in some way (for example kidnapping children) to send an apparently authorised wire transfer (Computer Fraud and Security Bulletin,1984b). Another way in which pressure can be brought to bear is blackmail.

Terminal access to SWIFT is controlled by a log-in system that requires a different password for every message transmission session. There can be several such sessions in one day. The passwords, 8 digits long, are sent to the bank in two parts on carbonized paper. In order to read the number the top sheet must be torn off. If the person carrying out this procedure thinks that the document has been interfered with then a set of contingency numbers can be used instead (Etheridge,1986). If three unsuccessful attempts are made to gain access to the network then a terminal is automatically removed from the system. Using mail to send out paper lists of passwords does make it possible though for these to be intercepted in the post and used by those unauthorised to do so. Moreover, whilst the password is divided into two sections, this is no protection against collusion.

Examples

1. Criminals were able to tap the lines used to transmit funds from banks in the United States of America to banks in Europe. Once a sufficient balance had accumulated in the European account instructions were then sent to transfer the balance to the criminals' own

account. US$900,000 was diverted in this way before the perpetrators were caught (Krauss and MacGahan,1979).

2. US$13.5 million was stolen from a Colombian bank by computer transfer. The secret codes required were somehow discovered by the culprits (Stanley,1984).

7.5.2.4.3 Fraud by staff at the sending or receiving bank

Members of staff authorised to initiate transactions are in a position to perpetrate a fraud and make payments to themselves or an accomplice. Improper operating procedures may also make it possible for other members of staff in the organisation to discover the requisite information (see example 3 below). A false instruction can also be inserted via secondary storage. Comer (1986) warns that particular care should be taken when a genuine message is buffered on to tape or disk prior to being read by the transmission systems since a false message can be created at this point. Finally, at the receiving bank a message has to be authenticated. It may be possible for a member of staff to simulate the arrival of a message, verify it and allow payment to be made. An employee may also deliberately ignore the fact that a message is not properly authenticated and approve the transaction. Many precautions taken to ensure the validity of messages are based primarily on the principle of the separation of responsibilities. It is common to allow one member of the sending bank staff to verify a wire transfer and another to release the transfer. These may be bypassed, however, by collusion between two or more employees. Employees, moreover, may well act with an outsider.

Examples

1.An employee of the City National Bank, with access to wire transfer passwords in connection with his duties as secretary to the Vice President, made fraudulent transmissions to the value of US$1.1 million. The money was used to purchase diamonds. The employee and his accomplice were sentenced subsequently to two years in prison (Norman,1983).

2.The Head of Slavenburg's Foreign Transfer Department was arrested on suspicion of obtaining tens of millions of guilders by fraud. It is believed that he transferred a large amount of money through a computerized banking system called AIMS and into SWIFT using codes given to him to carry out his job (Computer Fraud and Security Bulletin,1983b).

3. Stanley Rifkin, a systems analyst, entered the wire transfer room of the Security Pacific Bank in Los Angeles and observed how the staff assigned identification codes to authorised customers. Subsequently, he used this knowledge to transfer US$10.2 million to an account in New York. This money was then used to purchase diamonds in Switzerland. As he was foolish enough to return to the United States of America, he was arrested, tried and ultimately imprisoned for the crime (Norman,1983).

7.5.2.4.4 Staff employed by the wire transfer system

Members of staff often have the knowledge to initiate a false transfer, move an unauthorised transaction through the various processing queues, compromise test keys or complete a transfer prior to its checking by another member of staff. Again, collusion may be required for a crime to be successful.

7.5.3 Data manipulation

Data can be manipulated for the purpose of stealing funds from a financial institution. Fraud, larceny and embezzlement are all terms used, depending upon the circumstances, to describe the theft of money. These legal distinctions are not examined in detail since not only does the law differ from country to country but such niceties are not required for risk identification. As Wagner (1979) points out, the fraud techniques used are similar in nature to those employed previously in manual accounting systems. Computer crime can be committed more quickly, however, and there are no written records, only data that is invisible to the human eye. Both the entry of a false transaction or the alteration of a genuine one allows the illicit removal of funds. Several data manipulation schemes are described below.

7.5.3.1 Alteration of data input

Customer data can be changed at the point of entry, an unscrupulous retailer for instance might debit a customer account for more than the amount of the purchase. In wire transfer systems the name of the beneficiary, the dollar amount, the debit party or the credit party can be changed before, during or after transmission. Smart and Evans (1986) believe it is possible for criminals to misdirect large sums via EFTPOS to an existing account or one set up for fraudulent purposes. Then, making use of SWIFT, these fraudulently obtained funds could be transferred to a bank account in another country. It was the opinion of these authors that, at best, it would take time to identify and recover the funds and, at worst, the money might never be recovered. Programmers have the opportunity to alter the software in the host computers, network switches or the retailer's terminals to misdirect debit or credit transactions to or away from selected accounts or to destroy debit transactions. Attempts may be made to fraudulently apply transactions to inactive or dormant accounts.

Example

1. A programmer managed to obtain access to the front-end-processor of a banking system in order to divert 6 million pounds to his account in Switzerland by altering the payee number for the first ten transactions in an electronic funds transfer system (Wong,1986).

7.5.3.2 Alteration of messages

It is not only transactions that are transmitted along communication lines but also messages which authorize or reject them. If active wire tappers interfere with these messages with in some way a terminal can receive incorrect messages from the host computer or vice versa. Messages from the card issuers, such as stolen card information or transaction rejections, may be suppressed. If precautions are not taken, it is possible for someone to fraudulently simulate the host in ATM applications and send several authorisation to pay messages (Ritchie,1987).

7.5.3.3 Error correction

Errors are often made in data entry; upon discovery they have to be corrected by initiating adjustment transactions. In the absence of adequate controls, a dishonest employee can enter corrections where no error exists. A crime can be committed by submitting fictitious or improper adjustments. There are a variety of schemes depending on the application, the bank balance of the criminal can be increased by putting through a false ATM deposit; credit card accounts can be adjusted to indicate that a payment made was never recorded or a charge never made; a fraudulent message wire transfer may be inserted.

7.5.3.4 Changing files

The data files stored on disk or tape can be altered in order to commit a fraud. This can be done by altering, deleting or destroying transactions.

1. Alteration

   File maintenance transactions can be made that change the information such as a customer balance held on a master file. Other frauds include the alteration of credit limits of friends or fellow conspirators (so that they can run up large bills with no intention of making the required payment) and the modification of names and addresses on accounts prior to the re-issue of credit, ATM or EFTPOS cards so that new cards are sent to criminals and not account holders. It is not only the master files that are at risk. System information such as access control tables can be changed to allow a user greater rights than he was granted.

2. Deletion

   If the transaction file is modified prior to normal processing, transactions can be deleted so that they are not applied to the account. This is especially useful in the case of debit transactions, ATM withdrawals for example.

3. Destruction

   It is possible to make the data stored on disks or tapes unreadable, by overwriting or degaussing it for example. In this way evidence of transactions can be erased both on the database or log of changes (before and after image files). Computer staff may not do this voluntarily but be coerced, for example, by criminals into destroying EFTPOS transaction records and customer balances.

Many members of staff are able to interfere with data. Data entry and update clerks can change the direct access file data or the magnetic tape data by means of terminal entries or unit record entries whilst job set-up clerks who enter jobs and data into the job schedule can also modify or destroy data files. Others with similar opportunities include system

programmers and database administrators. In fact anyone who can find out the authorisation rights to data files can erase or change data including outsiders such as hackers if dial-up is available.

Example

The Computer Fraud and Security Bulletin (1985a) reported a case where an Italian bank was robbed of over £500,000. It was rumoured that the criminal was able to access and change computerized authorisation tables and messages awaiting transmission.

7.5.3.5 Data alteration during processing

The following strategies can all be implemented via unauthorised program modifications (Krauss and MacGahan, 1979) :

1. Breakage

   Breakage involves the siphoning off small amounts of money, rounding off amounts to the detriment of the customer

2. Undocumented types of transactions

   The criminal introduces an extra transaction type.

3. Balance manipulation

   A balance may have to be altered to cover up evidence of a fraud.

4. Deliberate misposting with lapping

   With deliberate misposting, either a charge is not applied to the correct account or the perpetrator's account is credited with monies due to another. Lapping is the process of deliberate misposting and the correction of this by another deliberate misposting to continue the fraud.

5. File modification

A program is used to make secret changes to transaction details in a file.

6. Fudging control totals

Fudging is a strategy that is often used in conjunction with another of the schemes described. Program code is altered so that the unauthorised changes are not reflected in the control totals.

7.5.3.6 Additional transactions

The criminal can enter an extra payment benefiting his own account. All of the banking applications are at risk. In credit card systems, a false payment may be made that clears a customer's debts, whilst in ATM applications and home banking fake credits can be put through. The refund procedure in EFTPOS systems, if it is available, is open to abuse. It generally requires the entry of codes known to certain members of staff but employees may misuse this information to make refunds to certain accounts and then withdraw the money from them (Johnstone,1985). Special facilities provided to train terminal users such as training mode in point of sale systems can be used to defraud employers. The terminal can also be removed from a retailer's premises and used at another site to create fraudulent transactions. Staff are in a position to enter extra transactions by the creation of fraudulent accounts. They can then divert money into these from valid (usually dormant) accounts. A Swedish bank employee transferred large sums of money to fictitious accounts over a period of five years by making false entries (Bequai,1987).

Of all the electronic banking applications dealt with in this thesis, wire transfer systems where large amounts of money are transmitted are most at risk. A fraudulent wire transfer might be sent through the system. In practice, criminals take advantage of public holidays in countries where the intermediary nodes for funds transfer are located. Messages have been automatically sent to their destination without checking (Comer,1986). The speed

with which such transfers are carried out enable the criminal to pick up the money before the crime is notified to the police.

Examples

1. Three computer experts were able to breach the controls on the ATM network and steal US$40,000. Initially they had no intention of stealing money but wanted to see whether they could defeat the bank's controls. Eventually they developed a system that allowed them to withdraw money even though the transactions were not recorded in the terminal's log (Bank Fraud, 1986b).

2. In 1983 the M19 terrorist group in Columbia syphoned off $13.7 million from the National Bank of Columbia by exploiting a weakness in the local telex system to direct a London bank to make illegal EFT transfers (Wong,1986).

3. Andre Prestes opened accounts with the First Variable and Virginia National Bank. His girl friend obtained employment with the First Variable and she wired US$1.55 million to Prestes' account with the Virginia Bank. This money was subsequently deposited in a Swiss bank account. The fraud was easy to commit. On a day when she was authorised to transmit 13 wire orders, Vera Compos, the girlfriend, included the extra transfer. Officials at First Variable only noticed the loss a month later but their lawyers tracked down the Swiss account and the funds were frozen. Prestes and Compos escaped to Brazil which has no extradition treaty with the United States (Bequai,1987).

7.5.3.7 Fictitious deposits

This fraud relies upon deposits that are not backed by funds. Either cheques are deposited that will not be cleared or fictitious deposits are made via ATMs (enclosing no cash in the accompanying envelope). Withdrawals are then made by criminals. The common fraud of kiting, obtaining money against uncollected funds, can be facilitated by making deposits and withdrawals via ATMs (Sauls and Towne, 1985). In some ways the

risks are lessened as the electronic processing of transactions means that there is no-one to become suspicious of a person making several trips to the bank.

Examples

1. This incident has already been used to illustrate the problem of staff error. However, it is also a classic illustration of a fictitious deposit. A fourteen year old boy declared a deposits of one million dollars (NZ) at an ATM but an empty Jaffa packet was placed in the accompanying envelope. The million dollars was actually credited to the boy's account. Subsequently he made several withdrawals, one for five hundred dollars. Eventually, the boy, who claimed to be experimenting only, told his teacher what had happened (Bell, 1986).

2. A 35 year old American was charged with felony after withdrawing US$495 credited to his account by false ATM deposits. Five deposits had supposedly been made to the total value of US$800, in all cases though the ATM envelopes were empty (Nilson report, 1987).

7.5.4 Collusion

The crimes outlined above are easier to commit when two or more people are in collusion. This gives the perpetrators access to more information as well as helping them to bypass the controls in place. Collusion is probably required between a retailer employee and a card holder to initiate fraudulent EFTPOS refunds since the staff member can provide retailer account information and access to the till. Bank employees who can discover account numbers and/or PIN information can sell their knowledge to criminals. In wire transfer systems, an outsider and employee can conspire to send a fake transfer or, if the staff responsible for initiating the transaction and verifying it are in collusion, they can alter a genuine transaction. As section 7.4 shows there are many errors which can be made that facilitate the execution of a crime. In order not to be implicated in a crime one or both of the parties concerned may claim to have made a mistake.

Example

1. An accounts clerk and a computer operator colluded in the creation of fictitious accounts. Money was transferred from valid accounts that had shown no activity for six months into a suspense account before being moved into the fraudulently opened accounts. In nine months, US$23,000 was stolen through cheques drawn on these accounts. By the time the fraud was discovered, 10 improper balance transfers a week were being made (Bank Fraud,1986a).

7.5.5 Taking advantage of a genuine error

There is the possibility in all electronic funds applications for funds to be erroneously credited to an account. A dishonest customer may not inform the bank when this happens. An Ohio man who instructed his bank to transfer US$774.75 to a new account at another bank found that he was credited with US$774,750.00. By the time the mistake was discovered the funds had been withdrawn and the customer had left the town. (Bequai,1987). A mistake of this kind occurs when data is inadvertently altered (either the account number or the amount), duplicated or misdirected. With wire transfer systems the amounts are so great that the recipient often absconds with the funds (Association of Reserve City Bankers,1983). On a smaller scale, cash in excess of the requested withdrawal amount may be disbursed by an ATM and accepted by the customer. One bank was fortunate when this occurred. The customer who intended to withdraw US$40 received US$5,140 but returned the money (Bequai,1987).

Example

1. A client of the United California Bank made a cable transfer from one account to another. The bank employee who handled the transaction transposed a single digit whilst entering the account number into the computer. As a result the amount was credited to the account of a self-employed bookkeeper. The bank did not realize that a mistake had been made because their books balanced but the error was eventually discovered by the client to whom the money should have gone. Unfortunately by the end of July the funds had been

withdrawn from the bookkeeper's account; US$600,000 was deposited in a Swiss bank account. The bookkeeper was found not guilty of grand theft after maintaining that he had mistakenly believed the money to be the payment of a fee (Norman,1983).

7.5.6 Falsification of data

Data can be inserted, altered or deleted maliciously in order to corrupt the data base or as a prelude to an attack on the system. In wire transfer systems, the deletion of a record can erase details of an authorised funds transfer. This deliberate destruction of a transaction will cause problems for the authorised recipient and the sender bank. The discovery that a file contains inaccurate data triggers error recovery procedures that might give a criminal the opportunity to carry out a fraud. It is also possible to change data such as access rights information to enable the commission of a crime. Finally, the log file that contains details of accesses to the database may be altered to cover up traces of a crime.

7.5.7 Suppression, alteration or destruction of output

The output, customer statements, reports or warning messages on a terminal, can be altered or suppressed. Incorrect customer statements may be produced to cover up evidence of fraud. Wong mentions that in some cases a Trojan horse program was used to suppress printing warning messages that alerted management to the fact that a crime was being committed. Exception reports given to management to review may be destroyed or amended to hide incriminating information.

7.5.8 Misuse of output

Computer output reports might be read to determine customer account numbers, dormant accounts, bank customer withdrawal patterns or any other information that might be needed to plan a crime. A competitor may also find a bank's reports interesting reading if statistics of ATM usage, volume of EFTPOS transactions etcetera are provided.

7.5.9 Unauthorised access

There are many ways that data can be accessed by those who have not been granted the appropriate rights. Information can be discovered directly by monitoring the radiation from a computer, wire tapping communication lines, illegally accessing the stored data (hackers or employees who browse and scavenge), printing out records or even by reading the impression on a printer ribbon. It is even possible for a maintenance engineer to take away a disk after a disk head crash and retrieve some of the data. During trials on the smart card, MasterCard discovered that the data in the chip could be read (Ladouceur,1987). Finally, at a conference held at Cannes, a Dutch security expert demonstrated that the information displayed on a VDU screen can be read by criminals equipped with a low cost receiver, amplifier and tuner to monitor the electromagnetic signals leaking from the terminal (Wong,1986). In this way, sensitive information such as passwords and account numbers needed to perpetrate a wire transfer fraud can be obtained.

Banks are very concerned about the deliberate disclosure of data that can result; it infringes either their own or their customers' privacy. In the first place, the release of financial information could have a detrimental effect on the viability of the institution. Secondly, a bank may be liable to civil or criminal penalties if the privacy of individuals is violated. Finally, information may be made available to criminals to help them to carry out a successful crime.

7.5.10 Extortion

There are various ways that a database can be endangered; criminals may be able to corrupt or erase the database. Beker (MacLennan,1987) mentions the possibility that criminals may threaten to destroy all the PIN information if they do not receive adequate payment. As he noted, this would cause the bank a major administrative problem as the replacement of cards and PINs requires a three year cycle. Alternatively, the removal of tapes and disks together with their back-ups might be sufficient to stop the bank

functioning. A company can be blackmailed in this way into paying out a large sum of money.

Example

In the 1970s ICI was the victim of a crime of this kind. An operations supervisor had access to tapes at both the main and back-up sites. He and his friend planned to steal the data and demand a ransom of £275,000. A total of 48 disk packs and 540 tapes were taken. Fortunately the perpetrators were caught trying to collect the ransom (Hayward and Kemp,1987).

7.5.11 Denial of valid transaction

In all the electronic banking applications dealt with in this thesis, it is possible for a customer who has made a transaction to deny that he was the person responsible for it. The customer may claim that the bank has made a mistake or that someone else must have obtained the required identification information and card (if needed). Generally speaking it is unlikely that a customer will meet with much success since the bank considers that if the transaction is authenticated in some way then it is valid. There are some problem areas, however. A card owner may claim that a card has not been delivered but has actually used it to make purchases or ATM withdrawals. It is quite difficult in this case for a bank to prove that the customer is lying. Disputed ATM withdrawals in the United States of America are resolved in favour of the individual if the bank cannot prove otherwise. To prevent customer fraud, cameras are often in place at ATMs and the photograph taken is stamped with the transaction number, providing a photographic audit trail (Crow,1982).

7.5.12 Theft of data

Data may be stolen from a bank for various reasons: to discover information for one's own use, to sell it to others (customer account numbers), to extort money from the bank or to sabotage the enterprise. Authorised database users can copy information and print it

out as can anyone else who has found out how to circumvent access controls. Alternatively, storage media can be removed from the library. Theft can be distinguished from unauthorised access in two respects. Firstly, the term theft involves the removal of the data from the premises. Secondly, an employee with access rights is just as likely to commit this crime (if not more so because of the greater opportunities available).

7.6 Sabotage

As mentioned previously sabotage may be the work of terrorists, a disgruntled present or former employee or even someone with a hatred of computers. An installation can be attacked in various ways in order to bring it to a halt, bombing and arson being the principle methods used. In the course of an attack the data stored on drums, disks and tapes may be destroyed. This is extremely serious if no back-up tapes are available or the data on them is out of date. The storage media can also be stolen to prevent the organisation from functioning. Sabotage can take place in less spectacular but no less damaging ways as well. A magnetic-tape librarian who lost her job replaced all of the computer master files with blank tape (Bequai, 1981). Critical data on disks can be removed by overwriting it with zeros or even by demagnetizing it.

7.7 Conclusion

Data is a resource that is obviously under threat from many quarters. In particular, a bank must protect itself from the introduction of a fraudulent transaction and the alteration of a data in order to commit a fraud. User authentication has been the subject of a great deal of research. The entry of a password or knowledge of a PIN does not allow a bank to check that the message was sent by a genuine customer. In this respect current smart cards are no safer than the use of magnetic stripe cards. People are still likely to note down PINs that can be discovered by a thief. Alternative authentication techniques that have been suggested are based on the physical characteristics of the user. Fingerprints and signature verification, retina scans and voice recognition are all being developed as means of customer identification. Clarke quoted an expert in this area, David Everett,

who stated that voice authentication was the most likely of these possibilities to be used in the future. As voice recognition systems are taking so long to develop, this might be a slightly optimistic view. He felt that a signature was too easy to forge, that fingerprints had a social stigma whilst "very few people like the idea of sticking their eye in a laser beam to test the retina print, even though there are no ill effects" (Clarke,1987). Whether banks are willing to make the necessary investment and convince the public of the advantages of these alternative methods of identification is another matter. It is not quite so easy to suggest a solution to the problem of the fraudulent manipulation of data as this can be done in so many different ways. Controlling access to the database is one measure that can be taken. Another is the establishment of a comprehensive audit program to ensure that data is protected at every stage of the processing cycle, input, processing and output.

Chapter 8

Threats to Communications

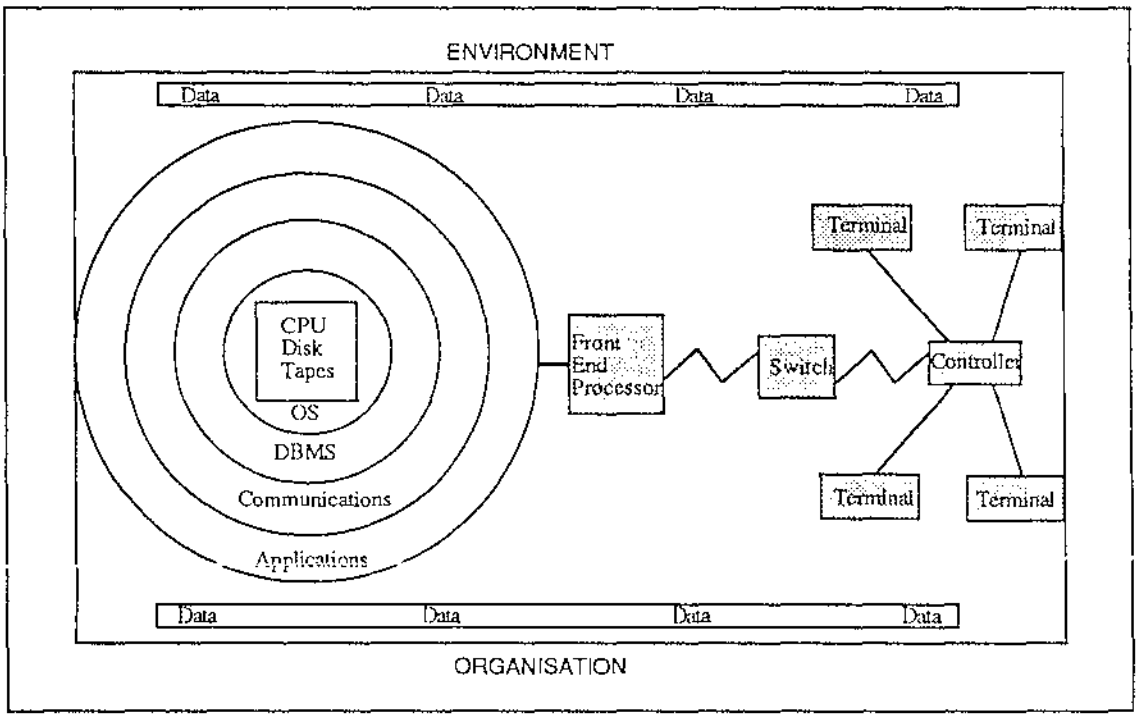


Figure 8.1 Communications

8.1 Introduction

In this chapter the threats to communications are identified under the headings of disaster, accident, error, computer abuse and sabotage. The risks inherent in the use of encryption are also examined. The communication system has three levels: the remote facility such as the terminal, the communications media together with associated equipment and the central computer system. Since the risks to the last have already been dealt with in chapter 4, no further mention will be made of this problem. The other components of the network can include terminals, modems, local area controllers, multiplexers, front-end processors, communication lines, security/line monitoring devices and transaction recording devices. The principle objectives of network security are operational reliability and the safety of the transmitted data. The former involves maximizing network availability both to meet customer needs and reduce the possibility of lost or erroneous transactions whilst the latter is concerned with protecting data from interception and modification. The main threats to these goals are equipment or transmission line failure and electronic crime such as active or passive wiretapping. Failure to counter these risks also exposes a bank to loss of business and loss of funds.

8.2 Disaster

The damage caused by a natural or man-made disaster can bring a network to a halt for several days if vital equipment or communication lines are affected. The duration of the shutdown will depend upon whether the network can be quickly re-configured and what back-up equipment is available. As with a hardware failure, the consequences of a shutdown may be disastrous if disaster recovery plans have not been drawn up and tested.

8.3 Accident

8.3.1 Equipment breakdown or fault

Equipment may breakdown due to a malfunction or wear and tear. Another serious threat to networks is a break in the communication lines, a cable may be cut through or brought

down in a storm. In the case where the component that has failed is not duplicated the network cannot be restored until the fault has been repaired and processing of transactions has to stop. Other consequences of the breakdown may include

- loss of the data being transmitted
- the misdirecting of a message
- the double processing of a message during the recovery process
- duplication of transactions. If a transaction is duplicated and processed twice then either a customer will suffer with a double debit to the account or a payment is made twice
- incomplete processing. If all the steps of the operation are not completed then incorrect records will be produced
- transaction delay. Transactions delayed at the input stage mean that there are also delays later on in the processing. The consequences can be serious in wire transfer systems
- transaction failure with loss sustained by customer

The problems just described are exacerbated in shared systems where a transaction may be switched through many networks. There are often technical problems with shared ATM and EFTPOS networks in the United States, most do not deliver more than 97% availability, if that, because there is always a weak link. Transaction completion can be denied due to network/host bank problems, " a situation all too common in a number of the U.S. networks" (Zimmer,1986).

An equipment malfunction might not be serious enough to cause the component to fail but could result in a faulty transaction being transmitted; a modem fault can mean that data transmissions are garbled or erroneous. Alternatively, a network might route messages to the wrong destination or deliver them late. Because of a temporary fault, such as a power fluctuation that affects transmission circuits, messages might be lost. The response

message to an ATM, for example, might not get through, the customer would not receive the cash even though the account was debited.

Locally, terminals can malfunction; in ATM systems in particular this is a problem. An ATM may not record deposits or withdrawals, funds in excess of the customer request or withdrawal limit may be disbursed or incorrect amounts for withdrawals recorded.

8.3.2 Noise on the line

White noise, impulse noise, crosstalk, phase jitter, envelope delay distortion and attenuation can all cause errors in data transmission (Stamper,1986). A single bit error can be important and change a request for $100 to one for $228. Since it is impossible to reduce all noise on the line, measures are generally taken to detect transmission errors. One of the most powerful methods, the cyclic redundancy check, is able to detect most mistakes. Retransmission of the corrupted block then follows. Forward error correcting codes which allow for the correction as well as the detection of errors are not suitable for the situation that often occurs in data transmission where bursts of errors occur.

8.4 Errors

8.4.1 Failure to provide adequate back-up

If critical components are not duplicated then an organisation may be able to offer at best a limited service (off-line rather than on-line ATM services) and, at worst, may need to close down. Duplication of critical components is not always a complete solution to the problem of network failure as Stephen Bell (1986) pointed out. There is a problem with a backup communication line if the common carrier puts the normal and backup link through the same cable. In New Zealand large users of data communications seek safety by leasing lines on two different routes. Whilst the two links might be separated when leased they might not stay that way if, during load re-distribution, the common carrier moves traffic from one line to another. Consequently, there is a substantial chance that when the main link is interrupted (perhaps damaged accidentally by a ditch digger for

example or even brought down deliberately for maintenance) the security backup will be in the same line as the main link. Whilst the New Zealand Post Office quote high figures for availability, 99.5%, the 0.5% of downtime may occur as a long break.

8.4.2 Insufficient capacity

A network might not have the capacity to support the volume of transactions transmitted. If this happens customer service is impaired (slows down or stops) because of traffic congestion. Whilst this might be an irritant to customers and retailers in ATM and EFTPOS applications, in wire transfer systems, the sending bank can be at risk because of the late receipt of covering funds resulting in a large intraday overdraft.

Example

The pre-Christmas demand on the Commonwealth Bank's automatic teller machine network was so great that it was out of action for forty minutes due to overloading. During the previous Christmas break the bank underestimated the demand for money from ATMs and some ran out of cash (Banking Technology , 1986a).

Wire Delays lose money

A recent report from the National Corporate Cash Management Association indicates that one in five corporations had problems with delays in funds sent over the wire network. If a firm does not receive a payment in time then it may have to borrow money to meet commitments. Several reasons were given for these delays - some banks computer systems are not able to cope with the volume of transactions so that there is a backlog in crediting transfers to individual accounts and other banks just have inefficient operating procedures. The Federal Bank regulations also exacerbate the situation since they limit the amount that a bank can be overdrawn. When a bank is too close to this limit it delays payments until its own funds position has improved (Pehrson,1987b).

8.4.3 Poor quality lines

There may be a problem with the quality of the lines provided by commercial carriers. In particular, since deregulation in the United States, the service there has deteriorated. Degradation of service has meant that messages are not always delivered on time (Shamoon,1986).

8.4.4 Omissions

Various measures should be taken to keep the network functioning correctly. These include physical access controls and an on-going and comprehensive maintenance programme. Problems are exacerbated in a shared network when it is also crucial to verify the identity of the sending bank. Omissions can occur in many areas :

- poor physical access controls allow intruders to enter the premises and damage or alter critical equipment
- poor monitoring and control. If diagnostic testing is not regularly scheduled, serious faults may go undiscovered, only surfacing when the network is brought down. The network operator should respond quickly and effectively to problems in order to maintain a 24 hour network service for ATMs and EFTPOS. Communication lines should be monitored for failures and traffic queues checked to detect bottlenecks. Unless there is this commitment, the use of the systems will be discouraged. Problems with the Trusteebank EFTPOS network in New Zealand highlighted deficiencies in N.Z.P.O Telecom's monitoring and control mechanisms (N.Z.Computer Scene,1986)
- inadequate measures to improve performance. Correcting a problem in one area might exacerbate a problem in another. In a case quoted by Stamper (1986), statistics showed that during busy periods the queue of transactions waiting for the ATM application was quite long. More ATM server processes were added to avoid long queues. Unfortunately this did not solve the problem; in fact statistics showed that the delays were longer

than ever. Insufficient memory caused an excessive number of page faults. Additional memory had to be installed to improve performance

- allowing the computer running the switch software to run other applications makes it possible for cross access to occur (Goldstone,1987)
- failure to test communications software thoroughly with the consequence that there is a temporary loss of service. During recovery, incorrect data may be accepted, transactions lost, sent to the wrong destination or processed twice
- failure to shut down the application when an abnormal condition is identified can have serious consequences. When ATM services were allowed to continue in off-line mode in Australia, many customers realized that it was impossible for the system to make the usual check against the customer balance. They took advantage of this to make withdrawals that left them overdrawn (Australian Financial Review,1987).

8.5 Computer abuse

8.5.1 Tapping of communication lines

One of the most serious threats to the security of data is the tapping of communication lines, either passive or active (Davies and Price,1984). Encryption and the use of message authentication codes (see section 8.7) provide some but not complete protection . It should be noted that encryption is not inevitably used. Whilst data is encrypted on the SWIFT network, there is no requirement for banks to be encrypt messages before entry to the SWIFT network at a regional processor. If no measures are taken to safeguard transactions and messages, wiretapping of one kind or another can occur.

8.5.1.1 Passive wire tap attack

A passive attack involves an attempt to read or store information being transmitted without altering it and is likely to be the prelude to an active tap. An unprotected line can easily be tapped; equipment can be connected that allows a tape recording of the digital data to be made. Radio and microwave transmissions, though, can be intercepted without requiring a physical connection. The terms eavesdropping and wiretapping are commonly used to describe the interception of data, whatever method is used to obtain it. In electronic banking wiretapping may take place in order to find out information that can be used later to carry out a crime. A traffic analysis attack, for example, enables an opponent to discover the frequency, length and origin-destination patterns of messages (Rutledge and Hoffman,1986). Transactions can also be monitored to obtain sensitive information such as account numbers and their associated PINs. Videotex which is based on the telephone services of the common carrier and generally uses dial-up lines is particularly vulnerable to attacks of this kind.

8.5.1.2 Active line tap

When an active line tap takes place, the criminal changes the transmitted data in some way. To operate an active line tap, the criminal must be able to persuade the devices at each end of the line that they are still communicating with each other. To put this more technically, the opponent must first interrupt whatever protocol is used to govern the transmission of data and then successfully mimic it, in order to convince the source and sink that they are still in communication with each other (Davies and Price,1984). Correct information flows to the active line tap whilst false information is transmitted to the front end-processor or host computer. Since communication lines are not always physically secure it is always possible that they will be tapped. When a terminal is inserted into the communication lines for this purpose, an active line tap is also referred to as piggybacking. The following exposures can result:

1. Alteration, deletion and addition of data

There are many ways in which fraud can be committed. Transactions can be altered so that the amount of a credit is increased, a debit decreased or a debit changed into a credit. Spurious transactions might be introduced. Finally, criminals might be able to interfere with the network so that credits are directed to the wrong account or debits are suppressed.

2. Changing the apparent origin

The source of the message is altered in some way, for example the terminal number is altered. Terminal identification is an issue of some importance in EFTPOS systems since retailers would not be happy if they lost their credits to others (Jacobs,1984).

3. Changing the actual destination - emulation of a card issuer's system.

Transactions might be re-routed to a dummy host computer centre which simulates the functions of the genuine host. This could accept fake transactions and generate apparently bona fide responses such as approval of ATM transactions that should be denied (Smart and Evans,1986).

4. Using previously transmitted or stored data again

Encryption and message authentication codes cannot prevent replay. Replay involves a criminal recording an encrypted or authenticated message and re-transmitting it later with the aim of making a second money transfer to a bank account. Whilst message sequence numbers can solve this problem, transactions employing a single message are more vulnerable. A sequence number can be allocated but the software will always have to make a check to see if a message has been duplicated (Davies,1984).

5. Falsifying an acknowledgement

Messages from the card issuers, such as stolen card information or transaction rejections might be suppressed (Smart and Evans,1986). If the system's remote terminals do not authenticate each message received with a message authentication code, a device can be connected on to the network that provides system-like responses (Ritchie,1987). For instance, a device called a spoofer can send instructions to an ATM to supply cash until the hopper is empty without any account being debited.

Example

John Webster, Chief Executive of the Homelink project, outlined the following scenario. "A disillusioned telephone/computer engineer digs a hole in the road and places a very powerful computer on the Homelink telephone lines so that he can collect signals from customers, de-code them and transmit them to us as if he were the customer - whilst simultaneously pretending to be the Homelink computer and telling the customer what he wants to hear. For example, the customer may be wanting to pay a bill to the Gas Board and the "hackers" computer has used the customer identification to instruct the Homelink computers instantly to transfer the whole balance of the account to the hacker, or someone nominated by him. Is this all too remote a possibility to worry about? Who would really bother to dig up the road, isolate the correct telephone line, create a very complicated software program, insert a computer to do all these things and risk being prosecuted too? If 10,000 accounts could be operated overnight, with instant fund movement occurring in millions of pounds, the answer is " A lot of people."(Webster,1985)

He believed that his organisation could counter such a threat but it might be that someone who knew the inbuilt security in collusion with the engineer could still carry out such a scheme.

2. The perpetrators of a US$900,000 fraud monitored wire transfers between two American banks and the European recipient of the funds. When the amount in the account was large enough, the criminals inserted instructions to transfer it to their own account in another European bank. One of the American banks discovered the wiretap in a routine inspection and alerted Interpol. The criminals were caught the next time they tried to move funds (Krauss and MacGahan,1979).

8.5.2 Masquerading

Unauthorised access to the computer is obtained by assuming the identity of a system user. The information required to successfully masquerade as a legitimate user depends on the particular application. In ATM and EFTPOS systems a card and its associated PIN are needed whilst a criminal has to obtain password and user identification codes in home banking and wire transfer systems. Wiretapping may provide the necessary codes. The masquerader can then send a fraudulent transaction if he has access to all the authorisation information. Dishonest retailers can install dummy terminals to capture card information and PINs. Such information could be used to generate large numbers of fraudulent transactions to their own account through a genuine terminal (Smart and Evans,1986).

The scale of the problem is immense. In electronic banking there are hundreds of thousands of terminals located in uncontrolled environments such as retailers' premises, homes, customer offices and inside the bank. The unauthorised use of these terminals is one of the greatest threats to security in on-line systems (Middleton,1986). If the transaction comes from an authorised terminal or local controller it may be accepted as genuine if the criminal can also provide the account number, password etcetera.

8.5.3 Between the lines entry

An unauthorised terminal is connected to a valid line and the felon then enters the system whenever a legal user (who continues to hold the channel) is inactive. The sign-off signal may be intercepted by the criminal and a fraudulent wire transfer inserted, for instance .

8.5.4 Browsing

Browsing involves linking an unauthorised terminal onto the system. A criminal who connects an unauthorised terminal onto the system might be able to browse through the database and find weaknesses in the system due to error, malfunction or poor security. Dial-up access to a database often provides a route for hackers into the system. Whilst leased lines are often used in banking, dial-up lines are used in home banking. It is possible for customers to access their data by dialling up the bank. If security procedures are insufficient then hackers may be able to browse through data or even alter it. Access to the dial-back security software can expose the security system to manipulation or the insertion of code modules that allow security breaches (Ritchie,1987).

Example

The following advertisements from America show the danger posed by hackers.

Computer Underground. Hacking, Crashing, Pirating, and Phreaking. Who's doing it. why they're doing it, and how they're doing it. Sample programs, phone numbers, and the tools of the trade.

Hacker's Handbook. Tells how to access remote computers, figure out passwords, access codes, operating systems, modem protocols. Plug into the electronic subculture; open up a world of new information (Risks-List,1987).

8.5.5 Emulation of equipment

It is a serious matter if a criminal can successfully emulate equipment, a terminal or controller, since the bank believes it is dealing with an authorised customer. A remote transaction can be sent from anywhere. Terminals, therefore, usually identify themselves to the system in some way, by a unique code for example. Since many ATM and EFTPOS systems use message authentication codes and encryption as security checks as well, it would be difficult but not impossible for a hostile terminal to convince the host computer that a message was genuine (Johnstone,1985). When the connection between a terminal and the computer is via a dial-up connection, however, there is a distinct

possibility that the terminal may be unauthorised. This is a particular risk with videotex terminals; true authentication cannot be conducted using dial-up lines since the real identity of the terminal cannot be ascertained and therefore the source of the call cannot be traced. Moreover, if a criminal is attempting to break into the videotex system then can he can keep dialling in.

In wire transfer systems, too, a fraudulent message may be sent from an unauthorised terminal. A bank employee with access to the cabinets that contain the communication lines and cables can connect up a line to an unauthorised terminal. Such a change can be made after a customer terminal was authenticated and allows the perpetrator to transmit an extra transaction.

Example

Two employees of Prudential-Bache initiated a whole series of fraudulent transactions from a personal computer at home. The authorised password unfortunately was well known to members of staff. Transactions totalling US$8.5 million were sent. Only a check at the last minute prevented a large loss to the firm (Wong,1987).

8.5.6 Disclosure of information

Radiation is generated by the components of the network. Devices are on the market that allow the radiation generated to be picked up. This gives criminals the opportunity to discover any unencrypted information that may help them carry out a successful fraud. It is also possible to misuse facilities such as a datascope. Datascopes are often used in communications so that the data transmitted along the line can be viewed. If unauthorised people access these they might obtain information that can help them commit a crime, passwords, message formats, account information etc.

8.5.7 Extortion

A threat may be made to bring the network down by terrorists, for instance, who claim that crucial components and back-up systems will be attacked if their demands are not met.

8.5.8 Attack on network components

Selected components of the network could be physically attacked so that the network would no longer function. This could be purely malicious in intent or be the prelude to a fraud. This might force retailers to switch to an alternative and possibly less secure method of authorizing and recording transactions.All the transaction records of selected retailers could then be stolen so that the customer accounts would not be debited (Smart and Evans,1986).

Example

At a security conference held in Auckland, Henry Beker reported that there was an organized crime attack on ATM systems where communications were disrupted forcing the ATMs to go off-line. Money was then withdrawn whilst authorisation checks could not be made (MacLennan,1987).

8.5.9 Taking advantage of on-going maintenance

In large systems such as the networks used for electronic banking, maintenance is often on-going leaving all of the components open to unauthorised access (Nestman, Windsor and Hinson,1984). Sometimes security measures, such as encryption, are switched off for a while. This gives criminals the chance to make unauthorised transactions or discover sensitive information.

8.6 Sabotage

Degradation or suspension of services can result from the following acts :

1. A home computer can masquerade as a retailer's terminal and be used to flood the system with a high volume transactions containing wrong PINs which might seriously degrade the service to genuine retailers (Smart and Evans,1986).

2. Selected components of the network can be physically attacked so that the network will no longer function. Action on such a scale would probably be the work of terrorists or highly organized criminals. Key communication links to leading stores can be cut,or powerful radio transmitters used to disrupt sensitive points in a network (Smart and Evans,1986).

3. Internal attacks on the installation and its associated components might be made by disgruntled or mentally ill employees. Again, terrorists or organized crime could be involved.

4. Host security modules can easily be sabotaged - a heavy jolt or the disconnection of a cable can cause the memory to be erased (Johnstone,1985).

5. Communication operators with access to the concentrators, multiplexers, modems, line switching units etcetera can bring the network down by overloading the data.They may also cause havoc by misdirecting the data. switching a message to the wrong destination for instance.

6. Computer vandals distributing thousands of pieces of electronic mail can cause a system overload. Alternatively the editor of the videotex system can be disrupted by continuous log on/log off sequences

7. An error can be introduced into the communications software by a programmer so that in certain circumstances the network fails.

8. Communication network managers can destroy the equipment in their charge (Bequai,1983).

9. Network messages can be interfered with so that genuine transactions are rejected (Smart and Evans,1986). This is not only inconvenient to customers but the bank might decide to shut down the network, believing it to be at fault.

8.7 Risks to encryption and message authentication

Where data communications are required for on-line processing of a transaction then data is transmitted in both directions between the source of the message and the host computer. At its most complex, this might involve a message being switched from a terminal to a mainframe via many other computers. Two methods are generally used to protect this data, encryption and message authentication codes. These procedures have been fully described in section 3.4. Key management and attacks on encrypted data are the principle problem introduced by the use of encryption. These threats are covered in great detail by Meyer and Matyas(1982), Davies and Price (1984) and in various standards. What follows is a brief description only of the major risks. As it is impossible to consider all encryption schemes, classical cryptographic systems like DES are assumed. Since public key is starting to play a larger role, however, this is briefly mentioned in section 8.7.5.

8.7.1 Banks and encryption

Banks have many important decisions to make about encryption - the algorithm to be selected, the method of using it, and its initialisation. There are many problems that have to be resolved if this process is to be successful. Keys and any initialising variables required have to be available both at the terminal and the cryptographic unit at the host computer that carries out the decryption. There may be a two or three key hierarchy used

by an organisation for data transmission purposes. In a two layer architecture the session key is used for encryption and MAC processing purposes during a particular time period, a day or a week for example. When this key is transmitted to the terminal it is encrypted by the master key. Another level of security is introduced in a three level system by the existence of a terminal key. The session key in this scheme is protected during transmission by the terminal key. Session keys, therefore, encrypt data whilst the master and terminal keys are used to transport keys through a network. There may be two session keys at an ATM or EFTPOS terminal, one to encrypt PINs and the other for use in the generation of message authentication codes.

8.7.2 Key management

The safety of all these keys is of vital importance to an organisation. A cryptographic facility, referred to as a tamper resistant security module is usually available at the host and terminals for storage. These modules are constructed with high quality physical locks backed up by systems that can detect interference. If an attempt is made to discover the keys then the unit is designed to destroy any important information, encryption keys or initialising variables.

If a bank using encryption has not put appropriate procedures in place to protect keys during transmission and storage then the organisation will be wide open to an attack through the unauthorised disclosure, modification, substitution, insertion or deletion of a key. In particular, discovery of the master key may involve its replacement in all the terminals in the system; a major undertaking. A key can be discovered or altered at various stages :

1. Key generation

   Before keys can be stored, distributed and used they must first be created. Meyer and Matyas (1982) describe various methods that can be used to choose master keys : tossing of coins, rolling dice or using a random number table. Other keys can be randomly generated so that there is an equal probability of choosing any of

the possible key values. When a random number or pseudo-random number generator is used though, the device might produce keys from only a certain range of possibilities. An opponent has the opportunity to predict a key value or find it through searching the keys with a higher than normal probability. Whatever method for key generation is used, if the proceedings take place in an insecure environment then keys can be disclosed, modified or replaced. The key generation algorithm or device can be modified or replaced in order to discover, alter or substitute keys.

2. Distribution and entry at a terminal

This distribution procedure is of crucial importance since the discovery of the master key allows the keys sent from the host computer to be decoded. If entry of the key is manual, no one person is generally entrusted with the complete key but it is entered under dual control. Distribution of the master key to terminals generally takes place by trusted courier(s). It is subsequently entered at the terminal by means of switches, dials, a hand-held loading device or keyboard by authorised personnel with access to the physical key(s) to the device. Cryptographic keys can be transported in hardware modules which make the keys inaccessible to the couriers. This makes it very difficult to obtain the key but it is not impossible. Plaintext keys that are delivered by courier should be under dual control to prevent disclosure but this does not rule out the possibility of collusion.There is also the possibility that for administrative convenience one person is given both parts of the key.

Terminal and session keys are usually distributed in an encrypted form on the communication lines but the following problems can still arise: a key can be modified, replaced or deleted during transmission to a terminal; a key may be discovered by an attack on the system as described in section 8.7.4 or the key could fall into wrong hands if interchange occurs before the other party is correctly

identified. There are obviously problems in distributing keys to a large number of EFTPOS terminals on retailer's premises.

False keys may be distributed or keys altered during transmission even though a terminal can verify the authenticity of a key. Incorrect keys can be distributed on a large scale to prevent the use of encryption on the network. If the bank believes it has a problem with key distribution, it may turn off encryption and allow plaintext messages to be sent (with the obvious dangers). The alternative, to hold up operations, inconveniences both the bank and customers alike.

Finally, in an ingenious fraud, an enemy terminal may pretend to be the communications centre and provide an ATM terminal with a session key that was used earlier but which the opponent has managed to decipher. With one criminal entering transactions at the ATM and another using the enemy terminal to send false authorisation messages, a considerable sum of money could be obtained.

3. Entry at the host

At some point in time a master key will have to be entered into the cryptographic unit in such a way that it cannot be discovered. If the key is read into the main storage of the host processor before being written into the cryptographic facility, it may be read from main memory or altered before the key value is cleared.

4. Storage in a cryptographic unit

Abbruscato (1986) notes that without physical access controls, "A bold individual (not necessarily a professional thief) can do more damage to the network's security by "borrowing" the key module for a short period than a cryptanalyst can do with a supercomputer over an extended period." Even the protective functions of the cryptographic unit - clearing of the key etc. might be circumvented by a clever criminal with time (for example someone who steals a terminal). Davies

and Price (1984) also mention that it may be possible to disable the protection provided for keys to allow the maintenance of the unit. This can give an opponent the chance to obtain the keys required. Certain cryptographic units are much more vulnerable than others, for example, EFTPOS terminals on retailers' premises and ATMs that are not located inside banks. If such an ATM is forced open and the decryption unit taken the keys and/or customer account and PIN information may be ascertained.

5. Key disposal

Poor methods of key disposal puts information such as PINs at risk.; discarded keys might be discovered and used to decrypt the data encrypted by them. In this way, if copies have been taken of ATM messages from the previous day or week, for instance, the PINs included in ATM messages can be obtained. Since the account number is in the clear, all the information may be available for a counterfeit card operation.

It is unlikely that the various banks in shared networks will use the same methods for verifying PINs so no single algorithm installed in an ATM or EFTPOS terminal can verify all the customer PINs. Banks are not likely to entrust other banks with their secret keys so generally verification is carried out centrally by each bank. All the terminals have to be on-line and connected via a network. Many messages are exchanged between the banks and these must be authenticated in some way; PINs may be carried from one processor to another. If a message is deciphered at a bank before re-encryption and forwarding to the card issuer then the message might appear as clear text - a procedure that makes a bank open to a fraudulent attack. Another risk is that a particular bank uses only one key to protect all its inter bank traffic; if this is discovered then the whole network is exposed.

8.7.3 Incorrect encryption

Even when all possible precautions have been taken the cryptographic unit at a terminal or the host may fail or malfunction with the subsequent loss of any keys stored there. Any keys lost will have to be re-entered into the device. In the worst case, a master key will have to be generated and subsequently distributed to all terminals. If keys have to be replaced in a hurry, the ensuing confusion might make it possible for an opponent to discover keys. It is also possible for encryption to proceed using the wrong key because of a hardware malfunction that changes a stored key. A software failure too can result in the incorrect operation of the algorithm or failure to use the proper key.

Mistakes can also be made that lessen the security in the system. Ritchie (1987) deals with the many errors that can be made :

- encryption keys sent in plaintext form through the network
- leaving a PIN to travel in plaintext form
- using a key prior to receipt of valid acknowledgments
- using a key when compromise suspected
- failing to destroy or re-using compromised keys.

8.7.4 Attacks on encrypted data

There are various ways that opponents can try to decrypt data.

1. Knowledge of the algorithm

   The first step has to be knowledge of the algorithm since it is very difficult to obtain the key when the encryption method is unknown.. This often presents no problem as many banks use publicly known algorithms such as DES. Others institutions though do keep the details of the algorithm secret and the criminal would have to obtain them in some way, possibly from disaffected employees. Once this knowledge has been obtained, there are various ways of proceeding.

2. Cipher-text only attack

In this case the criminal only has cipher text with no knowledge of the plain text. Davies states that it is impossible to find the key in this situation unless there is redundancy in the text but Meyer and Matyas (1982) state that a fragment of plaintext can usually be deduced from ciphertext because of the highly formatted text present in most messages and data files. The electronic codebook method, which involves dividing a message into 64 bit blocks and encrypting each one separately is especially vulnerable in these circumstances. Repeated phrases can be discovered that make it easy to obtain the key. Cipher block chaining, which involves using the output of one encryption step to modify the input of the next overcomes this problem. This makes the cipher block dependent not only on the plaintext from which it was derived but also on all the previous blocks. This makes it difficult to guess the key by analysing a group of messages.

3. Known plain-text attack

It is easiest to break a code where some plaintext and its equivalent ciphertext are available particularly when the plain text is generated by the criminal. Several transactions might be sent through the system whilst the line is tapped to secure the ciphertext.

4. Exhaustive search

The criminal attempts to find the key by trying all direct search methods. There are two ways of proceeding - key exhaustion and message exhaustion. With key exhaustion a known plaintext is encrypted with a selected key and the result compared with the corresponding plaintext. Each possible key value is tried in turn. This is likely to be a very lengthy process when there are a large number of possible values. It may be speeded up by using a computer but even then an estimate of the mean time to discover a 64 bit key when the key testing time is 1 ms and one key is tested at a time is over a hundred years. When tests are carried

out in parallel (1 million keys simultaneously) this still takes 107 days.(Davies and Price, 1984). A key exhaustion attack can also made if there is only ciphertext available. In this case trial keys are used to decipher the message; the output is checked to see whether it makes sense.

A message (or dictionary) attack takes place when an opponent knows an encryption key and uses it to encipher all possible cleartext message combinations. For example, there are only 10,000 possible combinations for 4 digit PINs, all of these could be stored together with their encrypted version. When a message is transmitted over the communication lines, the PIN can be recovered by searching the dictionary to find the plaintext equivalent. The message attack can only work if it is possible to encrypt and store all possible messages.

5. Analytical attack

An opponent solves a set of mathematical equations derived from the algorithm to obtain the key. To check that the correct key has been found, some plaintext and its corresponding ciphertext are required.

8.7.5 Threats to public key systems

Public key systems are often described as asymmetric as one key is used to encrypt a message and another to decrypt it. The encryption or public key does not need to be kept secret but the decryption or private key must be protected. Public keys can be used in various ways (Davies and Price,1984):

1. ATM network

With a secret key held at the centre and a public key stored at each ATM, the messages from the ATM to the host can be encrypted.

2. Shared networks

Each terminal can hold the public key of every issuer in the ATM network. If this becomes too cumbersome, a central authority can be established to hold the public keys of the banks. Customer cards contain the public key of the issuer. The ATMs store the public key of the key distribution centre and use this to check the validity of the issuer key before using it to code the request message.

3. A personal key approach using DES

In this approach each user's secret personal key is stored on a bank card and at the key distribution centre. These secret keys are used to distribute session keys throughout the network. The DES algorithm is then used for encryption and message authentication as previously described.

It is clear that the risks depend on the public key scheme used. Some general points can be made, however. When the transport of secret keys is avoided by the public key cipher there is still the risk that an enemy might be able to fool the user into using a key of his own choosing for which he knows the decipherment key. In this case the criminal who wants to maintain communication between the genuine sender and receiver has to decipher the message, re-encrypt it with the correct public key and transmit it to the relevant communication system.

The public key system might not be robust enough to make the guessing of keys impossible. If a criminal can make an educated guess at the contents of a message he can encipher it using the publicly available key to see if it is the same as the message transmitted along the line. In this way the right plaintext might be discovered; this could be very serious if session keys are sent on communications lines.

Finally, in some respects public key systems are no stronger than classical encryption algorithms : the secret key may be vulnerable at various points (generation, storage etcetera), incorrect keys can be distributed owing to noise on the line or interference from

criminals, and there is no protection against the modification or substitution of messages when public keys are easily available.

8.8 Conclusion

To meet customer and retailer needs, a high level of transmission performance is necessary; downtime has to be minimized to avoid inconveniencing them. It is also in a bank's best interests to keep the network running as this reduces the possibility of error and loss of transactions. To facilitate this, software and hardware faults must be reduced to a minimum. If the worst comes to the worst and the network does go down, then alternative communication lines and equipment should be available. In this eventuality the software should be able to cope with a temporary loss of service without any loss of data integrity. The widespread use of terminals and communication lines also provides the opportunity for electronic crimes such as wiretapping, masquerading and browsing. A network access control system can be set up to prevent hackers dialling into a network from their own terminal or personal computer. When the user dials up the mainframe, the call is intercepted by equipment which asks the user his password. The unit checks that the password exists, reads off the telephone number associated with it, terminates the connection and rings back the number corresponding to the password (Clarke,1987). The danger of altering messages in transit is so great that encryption and message authentication techniques have been introduced to combat it. This may be only a partial solution as it introduces problems such as that of key management and the selection of effective encryption algorithms. To reduce some of the problems of key management, Beker (1985) has developed a system using the DES algorithm where the key changes with each transaction. This may prove more secure than other encryption techniques.

Chapter 9

Threats to the Environment and Organisation

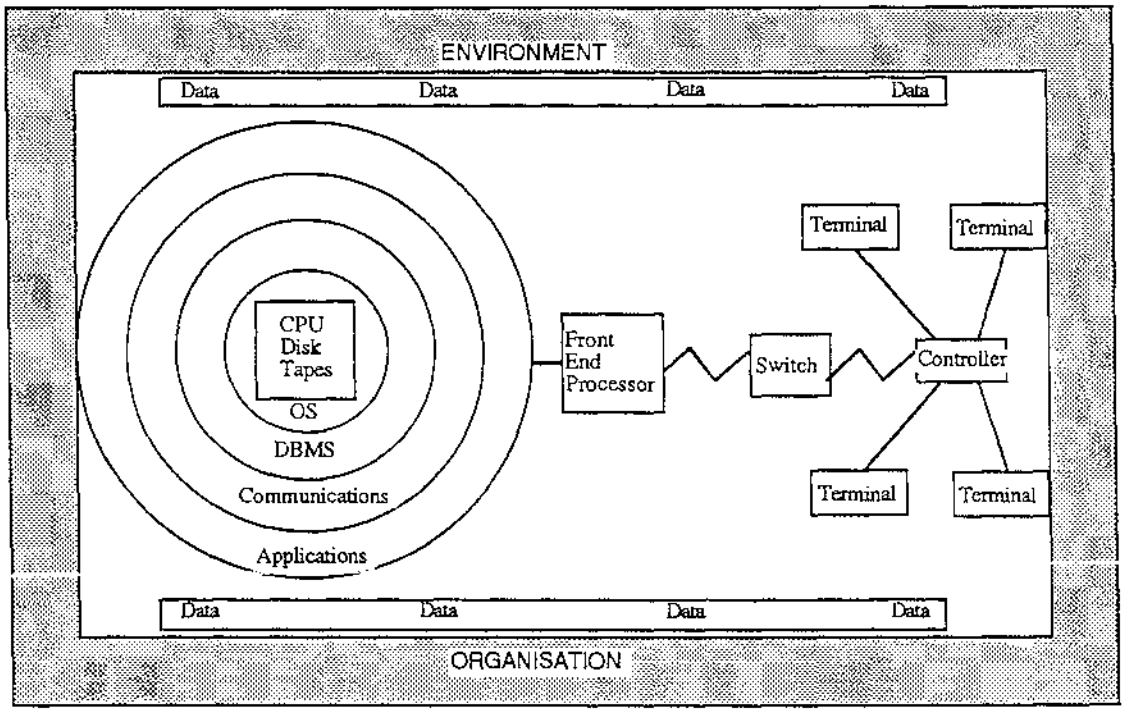


Figure 9.1 Environment and the organisation

9.1 Introduction

In this chapter the threats to the environment and organisation are identified under the headings of disaster, accident, error, computer abuse and sabotage. Some of the threats are wide-ranging such as risks to the support services (air-conditioning, lighting, heating waste disposal, back-up power and drainage) whilst others are application specific. In addition, there is a final section 9.7 which considers many of the broader organisational issues such as the implementation of security measures, customer privacy and the customer's legal rights.

9.2 Disaster

Man made and natural disasters that damage support services such as air-conditioning or back-up power can be as serious in their consequences as a failure of the hardware (see section 5.2). A pipe burst in the air conditioning which was fed from the Hudson river and the computer room on the 97th floor of the World Trade centre was flooded (Brown,1987). The accidental or deliberate turning off of the air-conditioning for instance can cause the computer to overheat preventing its continued operation. The consequences, in particular for wire transfer systems, can be potentially disastrous because of the large sums of money involved.

9.3 Accident

At a system level there may be a temporary loss of service due to damage to lighting, heating, air conditioning and back-up power.

9.4 Error

9.4.1 Omissions with regard to ATMs

Whether the ATM is positioned in the exterior wall of a bank or in a completely different location, it is extremely vulnerable to attack. Omissions of various kinds can make a crime relatively easy to commit :

- siting ATMs in insecure areas
- poor maintenance of terminals; the more unreliable they are, the more after hours maintenance is required with the increased possibility of theft either by the staff concerned or by criminals
- failure to check credentials of maintenance staff
- inadequate precautions taken to protect the environs, poor lighting of the area and an unsatisfactory alarm system put customers at risk
- failure to change regularly locks and combination of ATM safe
- single control to handle after-hours servicing
- electronics are accessible to bank employees, ATMs not repaired under strict control.

9.4.2 Unusable card

It is irritating to customers when their card will not operate a terminal or it is confiscated by the machine for no valid reason. Leiponis, the President of Electronic Money Services is on record as saying that ATMs occasionally capture cards for no reason at all whilst May of the Relay Network of California stated that 50% of one institution's ATM transactions were declined on the basis of incorrect PIN entry. It transpired there were encoding errors on the cards (Zimmer,1987). Brown and Brown (1986) state that the smart card is more likely than the magnetic stripe card to be unusable as a result of :

1. Manufacture when the card is exposed to heat and pressure.

   Heat is generated by the chip when it is in operation. The greatest build-up occurs during manufacture when the card is programmed. An excess of heat causes the chips to burn out. The power used by the integrated circuit chip is partly dissipated in the form of heat. PVC, used in the manufacture of these cards, is unable to evacuate the heat and may be deformed by excessive heat dissipation. This produces defects in the magnetic stripes and makes them unusable (Caillon,1985).

2. Embossing when the card is subject to physical pressure and heat.

The plastic of the card melts at the relatively low temperature of 50°C. The distance from the lines of embossing to the contact area and the chip location is often less than 3mm. The impact of the embosser, therefore, is enough to heat the card so that the plastic flows into the embossed character shapes. This leads to a high chance of damage to the chip. Moreover, if the card is left in an environment whose temperature is higher than 50°C, the card can deboss itself.

3. Improperly applied signature panel

If the signature panel is not properly applied then dirt and other particles can adhere to the contacts.

4. Glue

The card is attached to a mailer using adhesives and is then placed in an envelope, addressed, sent through the mail, sorted and handled. Contamination can occur if the glue used to affix the card to a mailer rubs onto the contacts or if any other dirt adheres to them during the delivery process.

5. Wear and tear

The card is kept in a wallet or purse and retrieved whenever a transaction is made. The dirt and dust in a wallet, purse etc. can contaminate the contacts of the card.

6. Faulty workstation

The smart card chip can be affected if the voltage applied to the contacts is above normal. Since the contacts require a different level of voltage to operate, a faulty terminal destroy a chip if the card circuits connected to the lowest voltage are burnt out by too high a voltage.

7. Electrostatics

The chip can be distorted or destroyed by large amounts of electrostatic activity. The normal build up of static activity in a house or the electronic signals of a dispensing machine with a smart card interface can cause this. If someone crosses a carpet on a dry day a spark jumps, the voltage is between 20,000 and 25,000 volts (Ladouceur,1987).

Research is being carried out to produce cards that minimise these problems. Mastercard carried out extensive tests on the smart card to check that it will have a reasonable lifetime (Ladouceur,1987). Nonetheless, it is likely that the smart card will be less reliable than the magnetic stripe card, particularly with regard to the effects of static electricity.

9.4.3 Failure to protect documents

Large quantities of documentation are kept to enable the smooth functioning of applications. These may include security and disaster recovery plans (Banking World, 1985). This information can be left around and made use of by those with criminal intention. Klein (1987), noted that in one money centre there were many safeguards against improper access to information but reports with the relevant information were easily obtained.

There is also the problem of disposing of documents. There are five ways in which sensitive documents can be destroyed : pulping, shredding, incineration, hammer mill and disintegration. All of these methods except disintegration have their problems. Shredding, incineration and hammer mill cannot be guaranteed to make the documents unreadable whilst pulping is suitable for only certain types of paper. Unless disintegration is used, therefore, there can be no guarantee that all important information has been safely disposed of. In one reported case, shredded cheques were re-assembled so that they could be processed (Hayes,1986).

9.5 Computer Abuse

9.5.1 Unauthorised use of sensitive documents

As described above in section 9.4.3 there are some very sensitive documents in the bank's possession, training manuals for instance. As well as these there is probably one copy of the bank's security controls and procedures and another of the disaster recovery plan as well as training manuals. These can all be used to provide the information that can lead to a successful attack on the system.

Example

1. Four conspirators decided to extort money from a bank by threatening to destroy the database. In order to do this they had to acquire information about all aspects of the bank's control system, the transaction trail and the structure of the files. One of the four conspirators worked at the targeted bank and he smuggled out, one at time, each volume of the bank's training manuals. The other three perpetrators each took one third of the document and photocopied it at their place of work. They eventually devised several methods of breaching the bank's access controls. Their inexperience showed, however, when the extortion attempt was made and they were caught by the FBI (Bank Fraud, 1987f).

9.5.2 Theft from an ATM

Incidents such as the following have led police to nickname ATMs "alternative theft machines" (Bequai, 1981).

- robbery of customers at an ATM
- robbery by servicing personnel during replenishment of the ATM, this is particularly likely when only on staff member is involved
- hold up and theft from servicing personnel
- the making of a false maintenance call in order to bring personnel to open up an ATM
- internal theft when counting deposits

- theft of ATM
- withdrawal of funds after account officially closed

Examples

1. A large Mid-Western bank lost US$440,000 due to single control access to the ATM for the purpose of servicing it (Ellis,1983).

2. In Melbourne, thieves used a stolen front-end loader to crash into the local bank. They then dragged an ATM through a glass wall, loaded it on to a stolen truck and drove it off to a rubbish dump where they proceeded to open the ATM with oxy-acetylene equipment. In this way they obtained $A60,000 (Banking Technology, 1986a).

3. Attack on service personnel

A bank employee who had gone to service a machine was found fatally shot in the head. The bank's policy had been to post the hours when the machine was closed for maintenance (Nilson Report,1987).

4. An ATM service team in San Leandro, USA was ambushed and US$68,000 stolen (Ellis,1983).

5. Money removed from ATMs

In Braintree, Massachusetts and Dallas, Texas money was removed from ATMs without any sign of forced entry. In the latter case, where US$7,200 was taken from an ATM operated by the Centennial National Bank, records indicated that the machine had malfunctioned. There was also evidence that the lenses of the security camera had been covered up. Other than this there was no evidence about how the crime was committed (Nilson Report,1987).

6. In Claremont, California, a man was robbed of US$200 after withdrawing the money from an ATM just before nine o' clock in the evening. His assailant, wearing a ski mask, threatened him with a revolver (Nilson Report,1987).

7.Thieves in New York bombed the Midland Bank's ATMs and stole US$10,000 (Bequai,1987).

8. Although the bank had instituted dual responsibility controls for the loading of cash in ATMs, the supervisor persuaded his companion, generally a uniformed guard, to stay with the car. The supervisor stole some of the money and covered up the evidence by tampering with the mechanism of these off-line units so that they would malfunction in various ways. At first the losses were attributed to problems with the terminals but eventually the security staff became suspicious and the supervisor was caught. By the time the perpetrator was caught, he had stolen US$32,000 (Bank Fraud,1987c).

9.5.3 False claim

ATM customers who have been physically robbed and assaulted have filed suit for damages. The total paid out in settlement to two of these customers was US$375,000 (Ellis,1983). There must obviously be the possibility of setting up such a scenario for the purposes of claiming damages.

9.5.4 Crime at off-line ATMs

Problems with off-line ATMs or on-line systems that are having to operate in off-line mode are inherent in the mode of operation and make life easier for the criminal:

- there is a longer time cycle than with on-line systems before notification of lost or stolen cards
- it is difficult to enforce rules regarding the number of withdrawals per day since this information on the card can be changed
- off-line status revealed by failure to give account balance.

Examples

1. Since ATM off-line systems cannot access customer balances, an Australian who had closed his cheque account was able to make a fraudulent withdrawal of $200 from an ATM. Subsequently he was convicted of larceny at common law (Tucker,1986).

2. In the United Kingdom, criminals used duplicates of a stolen card with a known PIN to withdraw cash from ATMs in the early hours of one week day when the central database was being updated and on-line access was temporarily withdrawn (Miller, 1983).

3. In New Zealand, a stolen customer ATM card was used to remove cash from machines at three bank branches . The money was taken from an account that was already overdrawn before the $10,000 was stolen. A daily limit of $150 dollars on withdrawals supposedly operated (Stanley,1984).

9.5.5 Vandalism

A raw egg thrown into a money machine in Palmerston North, New Zealand, put it out of action, causing NZ$1500 damage. Fluid from the egg seeped into the circuit board, shorting it (Evening Standard,1986).

9.5.6 Discrediting an electronic banking service

The Chaos Computer Club (CCC) found out the identification of another videotex user, a bank. The CCC set up a screen that was reasonably expensive to retrieve and then dialled up the videotex system using the bank's password and retrieved it 15000 times. The considerable costs for this were charged to the bank. CCC which aimed at bringing electronic banking into disrepute then announced that they had broken into a bank via Videotex (Maurer,1985).

9.6 Sabotage

Facilities engineers who check, adjust, repair, modify and replace equipment supporting computer and terminal facilities such as air-conditioning, power, lights, heat and water, can cause the air conditioning, backup power and lights to fail with the obvious consequences. Obviously uncontrolled entry to the premises by cleaning or security staff can increase such risks. ATM terminals located outside banks are easy targets for saboteurs. A civil rights activist was charged with attacking more than seventy ATMs with superglue (Computer Fraud and Security Bulletin,1985a).

9.7 Organisational issues

There are various organisational issues that need to be discussed in connection with electronic banking. Some of these relate to specific applications such as the problem of bankruptcy in wire transfer systems whilst others are concerned with matters that every financial institution should address such as the required level of security, the legal rights of customers, customer privacy, the impact of end-user computing and the danger posed by the accidental and deliberate acts of people.

9.7.1 Retailer problems with EFTPOS

If banks do not take account of the needs of the retailer then problems arise. Electronic terminals are probably also being used for other accounting and stock control purposes and need to be fully integrated into EFTPOS. Without such equipment retailers are

unlikely to give their full support to EFTPOS. The refusal by the system to accept a transaction in a supermarket after a trolley load of groceries has been registered would be a disaster as far as supermarkets are concerned. It may also prove extremely humiliating to the customer, particularly if the funds are in the account. The confiscation of a card by the system would also be very embarrassing (Cane,1986). Finally, in those EFTPOS systems where there is no refund procedure, the return of goods will not be easy to handle. A retailer might be reluctant to hand over cash to a purchaser until he is sure that the funds have been credited to his account.

9.7.2 Credit card losses

Svigals (1987c) reported that until 1985, the losses of the large companies in the United States of America were 1% on gross credit card sales. The controls over the issuing of cards were relaxed from 1984 onwards with the result that credit card losses climbed to over 1.4% of gross sales. This figure is expected to rise to 1.6% by 1990. Much of this loss is attributed to bad debts, which are projected to reach US$3.6 billion in the same year, and the remainder to fraud (see section 7.5.2.1). At the moment there are only limited checks to make sure that customers are not exceeding their limits. At busy times of the year such as Christmas, for instance, it may be impossible for a retailer to make an authorisation telephone call because lines are engaged. It is hoped that the introduction of smart card technology will solve this problem as a check can be made against the balance on the card. Cardholders should no longer be able to spend in excess of the limit and report that the card as lost or stolen (Burford,1986).

9.7.3 Bankruptcy in wire transfer systems

The possibility that the party sending the funds will not be able to settle is known as receiver risk. Receiver risk occurs in various (not Fed Wire) wire transfer systems and is so serious in its consequences that it must be discussed. It can happen as a result of an event external to the payment system such as the failure of a major bank or action taken by a state to impose exchange controls. Such an event could cause an unwise bank, one with

inadequate funds control procedures, to default on payments. Alternatively there may be a succession of participant losses which can result in the failure of a bank. There would also be corresponding losses for any participant in a net credit position with the failing bank (Association of Reserve City Bankers,1983).

In the United States of America the Federal Reserve Bank was very concerned about a systemic risk whereby the failure of one bank would lead to the failure of others in domino-like fashion. The Federal Reserve bank was so worried by the possibility that banks could not cover their overdraft position (termed a daylight overdraft) that it introduced controls to reduce the scale of the problem (Journal of Cash Management, 1985).

Daylight overdrafts occur in two ways. As banks transfer funds out in the morning in anticipation of receipts due later in the day then, essentially through timing problems in cash flows in and out of accounts, overdrafts are created. There are also banks that end the day with a Fedwire overdraft and cover their position by purchasing funds from the Federal Reserve Bank. With the repayment of those funds early the next morning, the banks concerned would have a daylight overdraft again (ABA Journal,1986b). The Federal Reserve Bank set limits, therefore, on the size of the overdraft that could be incurred in wire transfer systems. The amount is related to the bank's capital and is often referred to as a "cap". In addition, the Federal Reserve Bank stated that any private large-dollar transfer system that wished to be eligible for Reserve Bank net settlement had to require each participant to establish bilateral net credit limits vis-a-vis the other participants on the network and that there had to be some means of preventing payments that exceeded these limits (Cline,1986).

Instead of rigid regulations, it was announced that the banks would give themselves an appropriate rating ranging from "nocap" to "high cap". The self assessment process includes analyses in the areas of credit worthiness, operational controls and procedures,

and credit policies and procedures. Each one of these categories has scores associated with it. The three analyses are combined into an overall assessment, which is no higher than the lowest score in any one of the three categories. Table 8.1 shows how a bank comes to a single overall assessment. A problem with these controls is that they make the payment system somewhat inflexible. The disruption of service operation if banks withhold payments until the end of the day is known as "gridlock", that is the inability to send or receive funds because of the credit limit imposed either by the system or another participant. There are also implications for cash management. Banks need to be able to monitor their net position across all wire systems. The central bank has set up 4 categories regarding operational controls policies and procedures. For instance, to qualify for the top rating in this category the institution has to be able to monitor the position of 95% of all wire transactions every 15 minutes. Software changes will probably be needed to do this. There is another problem that the banks have to resolve - which customers will have priority when the overdraft allowed is almost exhausted. It is conceivable that no more transactions could be processed. This could give rise to subsequent legal problems. Banks are circumventing these controls to an extent by making more payments through the automated clearing house system. So far these payments are excluded from the overdraft arrangements as are government securities transactions. Since these accounted for about one third of all overdrafts before the limits were imposed, it can be seen that there is still the possibility that a bank could fail to meet its commitments. Moreover, the Federal Reserve Bank can only know after the event that a bank has exceeded its cap.

Credit Policies and Procedures	Operational Controls Policies and Procedures	Credit Worthiness	Overall Assessment
Satisfactory	Strong	Excellent	High Cap
Satisfactory	Strong	Very Good	Above Average
Satisfactory	Strong	Adequate	Average Cap
Satisfactory	Strong	Below standard	No Cap
Satisfactory	Satisfactory	Excellent	Above Average
Satisfactory	Satisfactory	Very Good	Above Average
Satisfactory	Satisfactory	Adequate	Average Cap
Satisfactory	Satisfactory	Below Standard	No Cap
Satisfactory	Unsatisfactory	Any	No Cap
Unsatisfactory	Any	Any	No Cap

From May,1985, the overall assessment translates into daily and two week average caps as follows :

	Single day Cap	Two Week Average Cap
High Cap	3.0 x adjusted primary capital	2.0 x adjusted primary capital
Above average	2.5	1.5
Average Cap	1.5	1.0
No Cap	0.0	0.0

Table 9.1 Cap Information (Cline,1986)

9.7.4 Security

A well known expert on security, Courtney (1986) believes that security measures are inherently undesirable. Not only do such measures cost money, they also impair performance and the usability of the system. To apply his arguments to electronic banking, a high degree of security can lead to significant transmission delays or a high rate of transaction rejection. Moreover there are no guarantees that the correct controls have been put in place. As Courtney (1986) says " There is no fixed set of controls, no beaten path, no yellow brick road down which you can go to the Good Witch of the South or at the end of which you expect to find adequate security." In the final analysis, the degree of security required in a system is a business decision. Banks have to trade off the costs of implementation against the losses before determining the appropriate level of security. When considering these losses, not only quantifiable risks must be included but also the possibility of failure of a bank as a result of a massive loss of confidence.

9.7.5 Legal Issues

This section mentions briefly some legal issues that have arisen with the introduction of electronic funds transfer systems. The American Electronic Funds Transfer Act is used as the basis for the following discussion as it provides one of the few legal frameworks for payment card transactions. The New Zealand Code of Practice is mentioned where appropriate (Ministry of Consumer Affairs,1987).

The purpose of the Electronic Funds Transfer (EFT) Act in the United States of America was to provide the framework for determining the rights, liabilities and responsibilities of participants in all electronic funds transfer systems except wire transfers (Le Clech,1987). A financial institution was to be held liable to a consumer for all damages caused by the financial institution's failure to make an electronic funds transfer, in accordance with the terms and conditions of an account, in the correct amount or in a timely manner, when properly instructed to do so by a customer. The institution is not responsible if action or

failure resulted from an act of God or if reasonable care was exercised (Marshall and Pylitt,1987).

Bequai (1986) pointed out that lawsuits can can arise from :

- how the data is collected
- the types of data that are collected
- the manner in which errors are corrected
- the persons who have access to data
- the way in which data is disseminated
- the measures taken to secure the system
- the time and manner in which notice is given to a customer concerning an error
- the legal duties and obligations of those operating the system.

It is not appropriate to look at all these problems but some of the more important ones are dealt with. An issue that has aroused much controversy is the resolution of disputed transactions. The EFT act in the USA states that only the institution that has access to the information can resolve the dispute (Tyree,1985). The EFT Act requires the institution to investigate and report in writing to the customer in the event of a dispute. If the customer does not accept the finding, he or she is entitled to access the documents used by the bank in reaching their finding. The onus of proof is on the banks. Based on this legislation, customer liability in the case of unauthorised transactions is limited to US$50 as long as a lost or stolen card is reported within two days. Not all nations have embodied customer rights in law, some such as New Zealand rely on a nationally accepted Code of Practice which provides for arbitration in case of a dispute (Ministry of Consumer Affairs,1987).

Banks have always been concerned about losses arising from customer negligence. Customers may lose cards, fail to inform the institution of the loss, write down the PIN or give their card and PIN number to a friend or family member. The Bankers

Association of New Zealand wanted all the liability for unauthorised transactions to fall on the customer when the cardholder was shown to be negligent but the code proposed that the penalty be the lesser of $250 or the balance of the account.

Violent attacks on ATM users, particularly at night, have received a great deal of publicity in the United States (Nilson Report, 1987). Some institutions initially refused to reimburse customers when the ATM buttons were pushed by the customer under threat but were advised such action was illegal. Some victims have sued banks on the grounds that all necessary precautions to provide a safe environment for customers were not taken. In two such cases compensation has been paid (US$375,000) although the settlements were out-of-court and no precedents were set (Ellis,1983).

Smart card disputes are particularly intractable as there is no hard copy of the receipt, just the record on the computer's files and the smart card itself. The validity of computer records in a court of law is a complex issue (see Tapper, 1983). Leclercq and Valbray (1985) mention that the lack of documentation causes problems since digital code can be a source of contention in the event that the card is used by a third party. What, for instance happens, if a criminal forces a customer to disclose the PIN? If the store and forward system loses the transaction as a result of a disaster, accident, error crime or sabotage, what procedures are in place to recover from this? Presumably, the bank will have to obtain information from the smart cards of its customers.

Bank fund transfer computer terminals are now placed with the customer. Anyone with a similar terminal and the authorised customer password could initiate transactions against that customer's account. Some banks have taken the position that if a customer employee exceeds his authority or if funds disappear from a customer's account via an outgoing instruction that they will not accept liability. A costly legal battle could ensue, however, if there is no agreement with a customer that lays down the conditions that have to be met before a bank accepts a transfer as being genuine (BAI, Funds Transfer Group,1984).

9.7.6 Customer privacy

Much customer information that is transmitted allows the identification of a user, the amount of the transaction and its location to be determined. Since privacy has recently become an issue of some importance the Standards Association of Australia concerned with the security of EFT (subcommittee IS/5/4) has now turned its attention to this topic. To date there is little customer protection in electronic banking. If information of this type is collated it could be used to track down the movements and financial dealings of an individual. Even the statistics of message traffic on a particular communications line can be useful. The ATM traffic on a line from a particular location may indicate the level of purchases in the shop and thus the cash takings (Caelli,1987).

9.7.7 End-User computing

Whilst all the major applications described in this thesis are developed by data processing departments or purchased from vendors such as IBM, there is an increasing trend for end users to develop their own programs or query a database using a fourth generation language (Hayward and Kemp,1986). Whilst it is not likely in banking that complex applications will be given to end users to develop, there are other possibilities. To carry out their departmental duties staff may write simple programs that interface with the bank's records or use programs such as SPSX to produce relevant statistics. Calculations can be performed using Lotus 1-2-3 and Multiplan on a personal computer (PC), again using the mainframe data as input. Expert systems may be developed to streamline administrative procedures; American Express have already set up a credit card authorisation program that obviously has to be linked up to relevant customer information (Louzoun,1987). Tellers are likely to be on-line to customer account information. Finally, staff members in the organisation may be able to use a fourth generation language such as SQL to interrogate the database of records. Rockart and Flannery (1983) estimated that 50% of all computing in the firms surveyed was user computing whilst Benjamin (1982) forecast that user computing will be responsible for 75% of computer cycles in many firms by 1990. Even allowing for the fact that banking is hardly a typical

commercial environment, the growth in user computing is so great that it must have a significant impact.

If an end-user is allowed to access the database from a terminal or personal computer, the bank markedly increases its security risks. In the first place, there is a great increase in the number of staff who are in a position by their accidental or deliberate acts to threaten the computer system. If care is not taken there may be a collapse of central control as computing expertise is dispersed throughout the organisation.

Worse still, an end user may perform the functions of a systems analyst, programmer and operator. There is no traditional division of responsibilities and there is in effect no check on the activities of such a person. Control over input, processing and output may be lost. Through inexperience the user may introduce mistakes into the database hence affecting its integrity. On the other hand, a user may deliberately try to defraud the bank by running his own program from a terminal. Information gleaned from conversations with data processing staff may provide information that allows the user to over-ride any operating system controls. A user may also be in a position to copy important information and take it out of the premises on a portable floppy disk. Finally, a disenchanted employee might deliberately introduce errors into the database (altering customer balances for instance) to cause problems for the bank .

End-user computing is of concern in electronic banking because its introduction puts customer and financial data at risk. As stated above it may also be possible for an end-user to manipulate this to steal funds from the bank. The only real solution is to set up an information database that contains the summarised information relevant to the needs of end-user departments. The system can be configured so that data can only be downloaded from the computer and not written back it. Even so the activities of end-users should be logged and monitored to make sure that they do not find ways round the controls.

It cannot be sufficiently stressed that if terminals or personal computers are connected to the mainframe in this environment, banks are greatly increasing their exposure to risks arising from the activities of staff.

9.7.8 People

People are of importance in computer based systems because their accidental and deliberate acts may threaten the organisation. It is people who make mistakes, commit crimes or sabotage installations.

Unfortunately there is an unlimited number of people who must be guarded against : programmers (application and systems), analysts, hardware engineers, operators, data entry clerks, media librarians, auditors, security staff, facilities engineers, end-users and outsiders such as customers, hackers or criminals.

The most important of these are the staff employed in the data processing department and computer centre; since they are essential to the functioning of the organisation they are thereby in a position to cause the most damage. Staff error is generally regarded as the single greatest risk faced by an organisation. With regard to computer fraud, the American Institute of Certified Public Accountants surveyed 9405 banks and 1232 insurance companies. (MacLennan,1987). It found that the most crimes were committed during normal working hours and that the most likely perpetrators include data entry clerks, computer operators, programmers and tellers.

Appropriate personnel practices should exist, therefore, to employ competent and trustworthy staff. Three other points need to be made, however. A problem that often arises in the computing industry is the loyalty of data processing staff to their profession rather than to the organisation that employs them. Friendships with the computing staff of other institutions may lead to indiscreet conversations, about weaknesses in the bank's computer system, for example. Employees may even decide to conspire with their friends to attack the bank in some way. This was illustrated by the case described above in

section 9.5.1 where a bank employee (a junior analyst) conspired with three other computer professionals to extort money from the bank. This can be countered by training programmes that make employees aware of their responsibilities to the institution.

Secondly, banking is vulnerable to the activities of both criminals and terrorists. Not only does it handle vast sums of money but it is seen by some as a symbol of the capitalist west that should be destroyed. Bribing employees is one of the ways that criminals and terrorists can use to achieve their aims. In fact, banking is an industry that lends itself to the corruption of employees as staff must always be aware of the difference between their salaries and the amount of money handled by the institution. The low paid, and often temporary, operators with the responsibility for running the computer are an obvious target for bribery. Such employees should be supervised properly. Providing staff with rewards in addition to salary (superannuation packages, loans at low interest rates) should also reduce this risk.

Finally, it is vital that the bank follow the well accepted practice of the separation of responsibilities. No individual should perform more than one function : the person who enters data should not verify it, a programmer should not be able to run programs. If duties are divided properly, it makes it more difficult to commit a crime since the collusion of at least two individuals is required.

It is impossible to estimate the total number of people who can threaten electronic banking in one way or another. Indeed the dimensions of the security problem are frightening. The widespread use of communications to provide services makes it difficult for a bank to exert the required degree of control. To end on a more optimistic note, it is possible for a bank to implement a well thought out programme of security measures and then encourage staff to support it. Customers, too, can be educated as to their responsibilities.

9.8 Conclusion

This chapter has focussed on environmental and organisational issues. Perhaps what should be stressed once again is the vulnerability of the mainframe. Even if it is only the support services that are affected initially, the system can still be put out of action for several days. Duplexing of sites is the only real answer to this problem. A bank also has to determine its responsibilities with regard to customer rights and privacy. A high-handed attitude to these matters (Pehrson,1986d) only alienates customers. Appropriate security and personnel procedures should also be established otherwise it is impossible to implement effective controls. Lane (1985) suggests many measures that can be taken including effective recruitment policies which involve formalized procedures for recruitment, assessment, training and termination. Finally, events such as equipment failure, computer runs from restart, failure of programs in operation as well as the usual details of program runs, files used should be logged. These journals should be scrutinized frequently and any irregularity discovered should be followed up.

Chapter 10

Conclusion

10.1 Introduction

"The World's bankers are beginning to learn what mischief they have let loose in opening the Pandora's box of electronic financial services. While they realize their competitiveness depends on the mastery of the new technology, they are weighing the advantages against what they now clearly perceive as disbenefits" (MacLennan,1987).

While some of the disbenefits refer to the cost of the new technology and its rapid development, others include the risks associated with the new technology. This thesis has sought to identify the security disbenefits or risks associated with the use of selected electronic banking applications : ATMs, EFTPOS, credit cards, home banking and wire transfer systems. It has not been possible to examine all variations of these services. Instead, for each application, a typical system has been described and used as the basis for risk identification. There is one exception to this, both on-line and off-line ATM systems were dealt with as the risks involved differ significantly.

Before considering the major findings of this thesis, some general comments can be made. There are obviously many variations on the threats described and they may appear in other forms than those found in these chapters. Furthermore, it is impossible to discover every danger to a system since criminals are only limited by their ingenuity. This situation is compounded by the fact that collusion between two or more people allows the circumvention of security controls. Finally, electronic banking has no national or international borders and network communicates with network. At the interface between these networks the conditions for fraud or serious error occur. Whilst each system may have appropriate controls in place, these may not suffice at the meeting point; a criminal may be able to slip through the cracks and discover ways of committing fraud. The introduction of international standards in an attempt to prevent this is a mixed

blessing, since sufficient information becomes readily available to those who wish to make an attack of some kind on the system.

10.2 Key risks

The risk identification process has drawn attention to the following issues:

1. Reliability and security

   The reliability and security of hardware, its associated support systems and the communications network is crucial in electronic banking. Computers, the telecommunication network and terminals are all vulnerable to equipment failure and sabotage. Moreover, communication lines can be penetrated to obtain confidential information, to corrupt or misdirect data and to alter transactions. Encryption and message authentication procedures to deal with these threats have their own problems, principally that of key management. Whether classical or public key encryption is employed there is always the requirement to keep the decryption key secret.

2. Authentication

   Personal identification and verification of customers or staff at a terminal is insecure whatever method of authentication is used. Cards of all kinds can be counterfeited whilst passwords or PINs that have to be memorised are relatively easy to discover. Since there are now large numbers of widely dispersed terminals linked up to a bank's computer the potential for abuse is great. Large sums of money can be stolen, particularly in wire transfer systems, if an unauthorised transaction is accepted. Cumulatively, losses from counterfeit cards can be substantial.

3. Error

   One of the standard slogans of the computing industry is "garbage in garbage out" (GIGO). Data can be incorrectly entered, altered in transmission (by noise on the

line or a modem malfunction) or improperly processed by software. Errors in a system, from whatever source, provide an ideal environment for crime. Other consequences include : the loss of funds; substandard, out of date, incomplete or inaccurate output; loss of confidence in the organisation; and the costs of a legal action. In wire transfer systems such risks are at their greatest with many of the recipients of erroneous transfers keeping the funds accidentally deposited with them.

4. Crime

Since banks deal with data representing billions of dollars they are obvious targets for criminals and terrorists. The system can be attacked in various ways. Data can be manipulated at the input, transmission, processing or output stages. There are many different schemes, of which a fraudulent or altered wire transfer message is the most serious, as huge losses can be sustained by a single transaction. Extortion is another matter of concern; financial organisations are asked to make a payment to criminals for some return such as information about a logic bomb that would erase the database. Finally, communications may be deliberately interfered with so that a bank moves towards a less secure mode of operating. Off-line instead of on-line procedures may be followed, allowing the withdrawal of large sums of money.

5. People

As the risks have been identified chapter by chapter, it has become apparent that the accidental and deliberate activities of people - customers, employees, hackers and criminals - are the principle threat to the security of banks. Indeed, it is almost a truism to state that security is essentially a people problem. Since computers depend on people for their operation and maintenance, software and data entry, this is hardly surprising. Employees can make mistakes, use the computer to steal funds or even sabotage the installation.

10.3 Countermeasures

Although primarily concerned with risk identification, this thesis has briefly discussed areas where countermeasures can be applied. If these were implemented they could greatly reduce but not eliminate the risks associated with electronic banking.

1. Alternative site

   If a bank is determined to continue processing whatever problems may arise, the only solution is to be able to operate from two sites (with the obvious implication that not only hardware but also software and data have to be duplicated). Any important network equipment should also be duplexed and, if necessary, arrangements made with the common carrier for back-up communication lines.

2. Physical access control

   Physical access controls can be grouped into three categories : perimeter controls, access controls to the data processing department, and access controls within the data processing department. Precautions are taken at each stage to make it difficult for an outsider to enter the computing facility. Possible measures include the surveillance of the entry lobby by closed circuit television, sign-in/sign-out procedures, escorts for visitors, the use of identification devices such as passes, voice or fingerprint identification systems, and the use of electronic key systems or badge reading locks.

3. User and employee authentication

   Biometrics, the use of unique physical characteristics as a means of identification, has been suggested as a technique that could find widespread application in banking. There are four realistic possibilities : signature, fingerprint, retina and voice authentication. Whilst the technology is available public acceptance is another matter. Naudts (1987), however, describes the successful use of fingerprint data by the Bank of America at its bank card centre in Pasadena. A

smart card contains a digitized version of an employee's fingerprints and this is compared with the fingerprint obtained from the fingerprinting device at the entry to the computer room. It can be seen that techniques such as these can easily be used both to identify customers at a terminal or employees at a bank's computer centre.

4. Software controls

Applications system development must be monitored at every stage of the software life cycle so that errors are not introduced into programs; a suitable methodology such as HOS can be used to produce provably correct code. Software should also have appropriate security procedures such as control totals and the advice of auditors should be taken early on in the proceedings. However, if controls are an afterthought and are not fully integrated into the software, they can be easily bypassed. Finally, opportunities to commit fraud and embezzlement during system development and maintenance must be minimized; system specification and design controls, programming controls, program change controls, and comprehensive program/systems testing must be implemented. Where error and fraud can be so expensive, it is essential to have such measures in place.

5. Encryption of data

Encryption of data is a useful countermeasure to the threats of passive and active wiretapping. The DES debate has shown technological advances may make current implementations of the algorithm obsolete. In the United States, the National Security Agency intends to supervise the development of algorithms that are more effective than the DES. Nonetheless there have been moves to continue the use of DES, though in a more secure manner

6. People

Adequate controls are needed to ensure that certain people (employees, terrorists, hackers, etcetera) cannot interfere in any way with the application. Each of the groups just identified has to be dealt with quite differently. Staff members, who cannot be expected to behave like machines may make mistakes as a result of inexperience, incompetence or negligence. Certain employees, systems programmers for instance, are particularly well placed to commit fraud or sabotage. In order to protect themselves against these dangers, there are many standard practices an organisation can implement that have proved extremely effective. These include vetting of personnel, adequate supervision of employees and enforcing the division of responsibilities.

Customers, hackers and criminals are not under the direct control of a bank and obviously have to be dealt with quite differently. The methods of combating them have already been described : a network access control system to thwart hackers, encryption and message authentication to stop fraud, smart cards with stored biometric information to identify customers, and physical access controls to prevent terrorists from entering the computer room.

10.4 Summary

Information systems, using sophisticated technology, are playing an increasingly important role in assisting banks to meet their corporate objectives. Much of this technology, it seems, has been introduced without full consideration of the inherent risks. In electronic banking, which involves the movement of money, the threats to security are considerable. With advances in technology, any poorly designed systems are likely to become more rather than less vulnerable over time. Technology, on its own, can never be a solution to security problems. Indeed, it only introduces a vicious and costly circle where more and more investment is needed to solve problems (including security) introduced by new technology. Instead, an appropriate risk management plan with the

full backing of top management must be drawn up and continually revised to take account of further technological developments. In this way the mischief unleashed by the Pandora's box of electronic financial services can be contained.

In the final analysis, perhaps banks should explore the implications of the new technology prior to implementing it. Ackoff noted as long ago as 1970 that the principle value of planning does not lie in the plans that it produces but in the process of producing them (Smith,1970). Banks should consider the problems carefully and decide whether they are ready to accept the risks borne by innovators in return for a strategic advantage. If they are, a preliminary review of the situation should identify obvious security risks that can be avoided. On the other hand, banks may decide to wait before introducing a service, implement a limited version or even ignore the area. Ultimately, this is a business decision as risks are balanced against benefits.

Appendix 1

Discovery of PIN

The major safeguard in card based systems is the fact that a transaction has to be authenticated by a PIN. The risks with regard to the unlawful discovery of PINs are twofold. Firstly, a person who obtains both a card and its associated PIN may masquerade as a legitimate user. Secondly, just discovering the relevant customer details and PINs allows determined criminals to perpetrate a counterfeit card fraud. On a small scale a considerable loss could be suffered by an organisation. If thousands of counterfeit cards were distributed, however, this would be much more serious. Such a crime might not be detected until the legitimate cardholders examined their statements or received notification that the account was overdrawn. The cost of this to a bank would be considerable. In the first place restitution would have to be made to defrauded cardholders if the bank wanted to retain their customers. Deciding which transactions were legal and which ones were fraudulent would be extremely difficult since customer declarations would have to be relied upon. In such circumstances, many people may make fraudulent claims on a bank either accidentally or deliberately. An important side effect of such a large scale counterfeit card fraud would be loss of consumer confidence in ATM and EFTPOSapplications.

To prevent such crimes the customer card and its associated PIN information should never be available together. There are three principle methods of generating PINS all of which have been described fully in section. Both randomly generated and, in some cases, customer selected PINs have to be stored on the computer system. To prevent personnel from accessing stored PINs, standards specify that these values should be held in an encrypted form. It is left up to the various organisations to decide whether the encryption is reversible or irreversible. With reversible encryption the system has the inherent capability of decrypting the stored PIN value and retrieving the clear text PIN. Reversible encryption is useful when periodically all PINs are decrypted and re-encrypted using

another key. This may be done regularly to prevent an adversary from compromising the current key. Reversible encryption also allows customers to be re-assigned the same PIN in the case where they have forgotten the value. Finally, reversible encryption provides for the decrypt and compare operation when PINs entered at an ATM terminal are verified. If irreversible encryption is used the PIN value received has to be transformed and the result verified by comparing it with the stored PIN value. The clear text PIN value cannot be decrypted, therefore, from the stored value. In the case of derived and possibly self-selected PINs the value may be stored on the plastic card.

There are six possible ways in which a PIN can be discovered for possible fraudulent use (Standards Association of Australia, 1985). This can be done via the card issuing institution, the PIN delivery system, the customers, the communication system, poor operating procedures and use of inadequate algorithms. All of these will be considered in some detail. To understand the following discussion, it needs to be appreciated that encryption keys can be used in many different ways :

- to generate derived PINs
- to encrypt stored PINs held on disk
- to verify PINs in off-line ATM systems
- to encrypt PINs for transmission to the computer.

1. The card issuing institution.

It may be possible to determine some or all of the PINs if an unsuitable method of producing derived PINs is used. Another danger arises if the PINs are generated from a cryptographic key. If a member of the staff obtains the key then all the PINs in the system will be compromised. Randomly generated PINs are open to different threats. No staff member for instance should be able to select the seed if a pseudo-random number generator is used to produce PINs. Any tampering with the random number generator can cause the range of assigned values to be greatly restricted and, thereby, more open to discovery.

Whether derived, randomly generated or self-selected, PINs, and possibly the related customer information, can be discovered by staff if management do not put appropriate controls in place. Risks are particularly great when staff have access to customer PINs (this may occur if customers mail or telephone their selected PIN to the bank), are allowed to change PINs or can find out the keys used to encrypt stored customer PINs. There are other dangers even if the envelopes are crash printed to ensure that no-one sees the PINs. It may be possible to read the PIN through the envelope or steam an envelope open. Should a breakdown occur when the envelopes are being crash printed, duplicate PINs may be produced after restarting the process. These may fall into the wrong hands. Finally PINs can be obtained via the hardware, software , recording media (disks and tapes) or paper (printouts and carbon) used during the generation, calculation or assignment of PINs.

2. The PIN delivery system

All banks that generate PINs have to deliver a printed copy to customers. The problem is compounded by the fact that the related cards also have to be sent. If cards and PINs are sent indiscriminately to customers who have not applied for this facility then unauthorised people often obtain them - this can occur because of a changes of address for example. Even when customers do request the card, PINs and the cards have been sent to the wrong address. Unless some procedure is set up to keep the cards and PINs separate then the risk of fraud is very high. Institutions have various ways of trying to ensure that the correct person receives both of these items and so guard against customer fraud. These are described below.

2.1 Mailing PIN and card

The PIN and card are produced at different locations and are both mailed independently to the same address. The major risk is that both of these items will be intercepted and used illegally by someone else. It is hoped that with two sites

involved the card and PIN do not arrive on the same day. This is one safeguard but of course it cannot be guaranteed. The card and PIN may be diverted in transit or may be taken by someone living at the same address. Unfortunately if customers have not been given a specific delivery date, they have no way of knowing whether the card and/or PIN have gone missing or not. In such circumstances, it is possible for a criminal to have two or three weeks use of a card before discovery of the fraud.

2.2 Collecting PIN and card from bank

The card and the PIN are kept in the bank and given to customers only after they have given proof of their identity. If the two items are stored together then members of staff could "borrow" them or could use the information in a counterfeit card fraud. To counteract this, the cards are usually kept in one locked location with one person responsible for them whilst the PINs are locked up elsewhere under the control of another staff member. This division of responsibilities will guard against fraud unless staff members are in collusion. Another danger is that in institutions that do not appreciate the need for security, one person, against all the rules is allowed full control.

2.3 Card collected from bank and PIN mailed

The authorised customer is required to collect the card from bank premises whilst the PIN is mailed to the customer address. This means that both items are never held in the same place until customers have them in their possession. Interception of one or other of these documents will have no effect other than inconveniencing the customer. Again, specially designed envelopes need to be used to ensure that the PIN cannot be read by an unauthorised person. Otherwise it would be possible for someone to subsequently steal the card from the appropriate address and use it to make a fraudulent withdrawal.

3. Customers

When criminals find or steal a card they often obtain the PIN. This may either be recorded on the card by the cardholder or on some document that came into the criminals' possession at the same time. It is the difficulty of remembering one or more arbitrary values that leads the owner to write the PIN down. The United States of America Justice Department report on ATM frauds in 1983 stated that in 72% of the cases where authorised transactions were made, the authorised user's PIN was recorded and kept near the card, typically in the owner's purse or wallet, or written on the card itself (Computerworld, March 18, 1985). The Arizona Bank conducted a survey which showed that a little more than 25% of returned or captured cards had the PINs written on the signature stripe (Ellis, 1983). PINs can also be discovered in other ways. A customer may fail to destroy or secure the PIN envelope or divulge the PIN to someone else, either intentionally or as a result of trickery. PINs may also be ascertained by observing entry or selection at a terminal. A casual passer-by, a determined criminal who trains a closed circuit camera on the PIN pad or a sharp-eyed cashier in a bank are all able to do this. Finally, customer selected PINs are open to discovery by guesswork since an easily remembered combination such as a birth date is often chosen. Someone using personal knowledge of the cardholder, perhaps obtained from a stolen diary or wallet, may be able to work out the PIN. A study in the United States have shown that only 15 common words comprise 80% of all customer selected PINs (Streeter, 1982). Since many people now possess several cards, the threats to PIN security are magnified. If a different PIN is associated with each card, the difficulty of remembering many PINs forces customers to record the PIN with the card. When the customer is able to select the PIN, though, he may decide to protect all his cards with just one PIN. Once this has been discovered, using one of the methods described above, anyone who obtains the PIN and the cards will find that they have access to several accounts.

4. The communication system

4.1 Wire tapping

Unencrypted or improperly encrypted PINs can be discovered from taps on the appropriate communications line when PINs are transmitted to the computer for authorisation.

4.2 Staff activities

If a program exists to decrypt or encrypt the stored PINs after they have been moved into main memory then they can easily be compromised. PINs may be obtained from the buffers if these are not cleared immediately. Alternatively, the software could be tampered with by a programmer to allow a member of staff to print out the PINs and associated customer information. As serious is the danger that a staff member may discover the cryptographic keys used in PIN storage. If the same person or another acting in collusion acquires the file of PINs stored in the system then all the values will be obtained if reversible encryption is used. Even when irreversible encryption is used a staff member could obtain the encrypted PINs from disk or tape and alone or with others employ crypt-analysis techniques to discover them. If production data is processed by encryption devices containing test keys or test data is processed using production encryption keys then it is possible to conduct an attack on stored encrypted PINs. (Ritchie,1987) Staff members in the computer centre, the library of secondary storage, the data processing department or the site where backups are held all have some opportunities to compromise PINs.

4.3 Terminal tapping

The PIN keypad in the point-of-sale environment is not very secure. It may be possible to tap the keypad and record all the PINs entered or even to discover the keys stored there and use them to decrypt PINs in EFTPOS messages. (Johnstone, 1985) The customer identification information which is not encryped

can easily be obtained by tapping the communications lines. Fraudulent cards can then be easily manufactured.

4.4 Fake equipment

Fake equipment to capture PIN information can be put in place. Dishonest retailers can install dummy terminals to capture card information and PINs. Such information could be used to generate large numbers of fraudulent transactions to their own account through a genuine terminal or to use the information in the production of fraudulent cards. (Smart and Evans, 1986)

5. Improper operating procedures

Loopholes in operating procedures may be exploited. If customers are permitted an unlimited number of attempts at PIN entry for example then it is possible to obtain the correct PIN by trial and error. Another weak point occurs when customers are permitted to use a terminal on the bank's premises either for the initial issuing of a PIN or to alter its value. There is always the possibility that the person asking to select or change the PIN is not the legitimate owner of the ATM card. Checks need to be made with regards to the identity of the customer; the machine should only be operated by an authorized employee who can identify himself to the system and, after the PIN selection process is completed, the terminal should be logged off. If any of these steps are omitted then there it will be possible for someone to obtain a PIN unlawfully. (Unfortunately in the case where a bold criminal has obtained a wallet with several identifying documents this will not be sufficient to prevent someone from masquerading as a customer.) Similarly, stringent precautions are required if PINs are selected at an unattended terminal or issued by mail or phone. In the circumstances where a customer returns a card and PIN then there should be different return addresses. This does not preclude, however, a customer returning them together.

Cards that are stolen should be captured by the machine. This can be achieved in two ways - the ATM takes possession of the card if it is reported stolen or if the incorrect PIN is entered more than a specific number of times. No one person should have access to these captured cards have been misused by bank employees (Khanna, 1985).

6. Weaknesses in the encryption process

Secure encryption depends upon the choice of a good algorithm and effective key management procedures. Since in off-line ATM systems the master key is required for PIN validation, its discovery threatens the security of all the PINs in the system. Similarly, the compromise of the key used to encrypt transmitted PINs allows for their decryption. The issue of key management is dealt with more fully in section. Ritchie (1987) discusses some other problems that arise from the improper use of encryption. In particular, PINs can be discovered if they are stored in plaintext form in the terminal, travel in plaintext form between an EFTPOS terminal and a terminal controller or are processed accidentally as data requiring message authentication thus leaving the PINs in the clear.

Appendix 2
Glossary

Acoustic Coupler. A device that converts electrical signals into audio signals, permitting transmission of data over public telephone lines.

Acquirer. The institution, or its agent, which acquires, from the card acceptor, the financial data relating to the transaction, and which initiates that data into an interchange systems.

Algorithm. A clearly specified mathematical process for computation; a set of rules which, if followed, will give a prescribed result.

Alphanumerics. Characters consisting of letters, numbers, and, sometimes, symbols.

Application Software. Computer program designed to accomplish a specific task

Attenuation. This is the weakening of a signal as a result of distance and characteristics of the medium.

Audit Trail. A printed record of transaction listings created as a by-product of data processing or mechanized accounting operations.

Authentication. The act of determining that a message comes from a source authorized to originate messages of that type and that the message is as authorized.

Authorisation. A security process to decide whether a service can be given or not.

ATM (Automated Teller Machine). Self service system offering a variety of transaction possibilities activated by card (including cash withdrawals.)

Auxiliary Operation. An operation performed by equipment not under continuous control of the central processor.

Binary Code. A code using two distinct conditions, usually 0 and 1.

Bit. The smallest unit of information in a binary system of notation.

Block encryption. The technique by which 64 bits of clear text are encrypted to yield 64 bits of cipher text.

Cap. The daily overdraft limit allowed a bank by FedWire.

Card acceptor. The party accepting the card and presenting transaction data to an acquirer.

Card issuer. The institution, or its agent, which issues the identification card to the cardholder.

Cardholder. The customer associated with the Primary Account Number (PAN) requesting the transaction from the card acceptor.

Cipher text. Clear text that has been encrypted.

Clear text. Intelligible text or signals that have meaning and that can be read and used.

CPU (Central Processing Unit). The unit of a computer that controls the interpretation and execution of instructions.

Common Carrier. A regulated public utility, such as the telephone company, which provides communications services.

Crosstalk. This occurs when signals from one channel distort or intefere with the signals of a different channel.

Data Acquisition. Identifying, isolating, and gathering source data to be centrally processed in a usable form.

Data Centre. A computer-equipped central location.

Debit Card. A card used to create debits in a customer account. It may be used to activate an ATM.

Decryption. The transformation of cipher text into clear text, sometimes referred to as decipherment

DES (Data Encryption Standard). An algorithm used for encrypting and decrypting data.

Encryption. The transformation of clear text into cipher text for the purpose security or privacy, sometimes referred to as 'encipherment'.

Encryption algorithm. A set of mathematically expressed rules for rendering information unintelligible by effecting a series of transformations to the normal representation of the information through the use of variable elements controlled by the application of a key.

Envelope Delay Distortion. This occurs when signals that have been weakened or subjected to outside interference by transmission over long distances are enhanced by passing them through filters.

Financial institution. The institution responsible for the custody, loan, exchange, or issue of money; for the extension of credit; and for facilitating transmission of funds.

Hardware. The physical equipment involved in electronic data processing.

HOS (Higher Order Software). A software development methodology which integrates proofs of correctness.

Host Computer. A computer attached to a network and providing services, such as computation, data base access, or special programs.

Identification. The process of associating a unique characteristic to an individual.

Impulse Noise. The noise which is produced by electrical impulses on telephones which is heard as a clicking or crackling.

Input Process. Information transferred from an external source to internal storage in a data processing system.

Integrated Circuit(s). Electronic component(s) designed to perform processing and/or memory functions .

Interchange. The mutual acceptance and exchange of financial transaction messages.

Interface. The connection between two systems or two devices.

Irreversible encryption. The transformation of clear text to cipher text in such a way that the original clear text cannot be recovered by other than exhaustive procedures.

ISO. International Standards Organisation.

Key. A secret number or character sequence that governs the enciphering or deciphering of information.

Line Encryption. The cryptographic processing of data before its transmission from one point to another.

Master Files. The overall mass of records containing all relevant information in connection with an account or a customer.

MAC (Message Authentication Code). A code in a message between the sender and the receiver used to validate the source and part or all of the text of the message. The code is the result of an agreed calculation.

Microcircuit Card. A microcircuit card is an ID-A card type into which has been inserted one or more integrated circuits.

Modem. A device that, in effect, translates data signals from one format to another, as from data terminal format to telephone system format and vice versa.

Off-Line. Equipment or devices not under the control of a cental processing unit or controller.

On-Line. Equipment or devices under the control of a central processing unit or controller.

Offset. A number that mathematically relates a calculated identification code to a customer-selected PIN.

Parity. A measure of the number of '1' bits in a group of '0' and '1' bits.

Parity bit. A bit added to a group of '0' and '1' bits which may be used to make the parity of the group, or extended group, odd or even.

PIN (Personal Identification Number). A numeric or alphanumeric code or password that the cardholder possesses for the purpose of identification.

Phase Jitter. This is the variation in the phase of a continuous signal from cycle to cycle.

PIN assignment. The process of establishing the relationship between customer authentication and customer identification data.

PIN issuance. The act of conveying PIN information to a customer.

PIN offset. The number that mathematically relates a calculated identification code to a customer selected PIN.

PIN verification. The act of verifying a customer's authenticity by the issuer.

POS (Point of Service) . The location where a transaction is originated.

PAN (Primary Account Number). The card-holder's card number including the information identifying the issuer to which the transaction is to be routed.

Program. A set of instructions that directs the computer to perform a specific task or series of tasks.

Protocol. A formal set of conventions concerning the format and relative timing of message exchange between two communicating processes.

Pseudo-random. Virtually unpredictable though not statistically random.

Random. Haphazard, unpredictable

Real Time. The processing of data quickly enough to make it available in time to influence the process being monitored or controlled.

Reversible encryption. Transformation of clear text to cipher text in such a way that the original clear text can be recovered.

Software. Programs written to direct a computer to perform specific functions usually categorised as system, database, communications and application software.

Transaction Limit. The maximum amount of a single transaction that can be authorised within a given application data field.

Validation. The process of proving the integrity of a message,or selected parts of a message.

White Noise. The noise produced from the movements of electrons which is present in all transmission media at temperatures above absolute zero.

Bibliography

ABA Banking Journal, 1986a : What will S.W.I.F.T. II mean to your bank ?, ABA Banking Journal, September 1986, pp.44 - 45

ABA Banking Journal, 1986b : Purging risk from the payment system, ABA Banking Journal, September 1986, pp.136-138

Abbruscato, C.R., 1986 : Choosing a key management style that suits the application, Data Communications, April 1986 pp.149-160

Aguilar, Ronald J., 1985 : Secure protocol set for a multi-level-secure LAN in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Akl, Selim G., 1983 : Digital Signatures : A Tutorial Survey, IEEE, February 1983 pp.15-24

Alagar V.S., 1986 : A Human Approach to the Technological Challenges in Data Security, Computers and Security, 5 (1986) pp.328-335

American National Standards Institute, 1982 : Financial Institution Message Authentication, ANSI X9.9

Anderson, R.E., 1981 : Bank Security, Butterworth Inc, Woburn, MA.

Anderson, Robert G., 1987 : The Destiny of DES, Datamation, Vol.33 No.5, pp.79-84

Andrews, Martyn, 1985 : LAN security for different threat environments in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Association of Reserve City Bankers, 1983: Risks in the Electronic Payments Systems, Association of Reserve Bankers

Athanasiou, Tom, 1985 : DES Revisited, Datamation, Vol.31 No.20, pp.110-114

Avadian J.H, 1985 : Bank Card Fraud and Credit Loss Controls in Smart Cards From France to the World, Editor Louis-Noel Joly, Lafferty

Bailey, John, 1986 : EFTPOS - The Westpac Experience and Other Developments in Australia and the Far East presented at EFTPOS & Home Services, 1986 International Conference, Edinburgh, November, Paper 6

BAI Funds Transfer Task Force, 1984 : Process and Control Guidelines for Wholesale Funds Transfer Systems, Bank Administration Institute, Rolling Meadows, Illinois, 1984

Bank Administration Institute, 1983 : ATM Security, Bank Administration Institute, Rolling Meadows, Illinois

Bank Fraud, 1986a : Case 86.002 - Collusion and the Computer : A Dangerous Pair, Bank Fraud, Vol. 1 No. 1, pp.5-6

Bank Fraud, 1986b : Case 86.008 - ATMs Are Easier to Steal From Than People, Bank Fraud, Vol. 1, No. 3 pp.4-5

Bank Fraud, 1987a : Case 87.007 - Ineffective Controls Are Quite a Temptation!, Bank Fraud, Vol.2 No. 2, 1987, pp.5-7

Bank Fraud, 1987b : Red Flag Warning - How to Detect Potential Fraud and Insider Abuse Situations, Bank Fraud, Vol. 2 No.4, 1987, pp.3-5

Bank Fraud, 1987c : Case 87.011 - Don't Worry. It's Just a Glitch!, Bank Fraud, Vol. 2 No. 5, 1987, pp.1-2, 8

Bank Fraud, 1987d : Risk Management Situation 87.4 - Cutting Your Credit Card Risks, Bank Fraud, Vol. 2 No. 6, 1987, pp.4

Bank Fraud, 1987e : Case 87.013 - Create a Caesar's Wife and Fraud May Be A Companion, Bank Fraud, Vol. 2 No. 7, pp.1-3

Bank Fraud, 1987f : Risk Management Situation 87.7 - Misuse of Banks Manuals to Extort Funds from Institutions, Bank Fraud, Vol.2 No. 7, pp.4-5

Bank Fraud, 1987g : Spotlight On ATM Fraud : Crime Ring Discovers System's Soft Spot, Bank Fraud, Vol. 2 No. 8, p7

Banking Technology, 1984 : The Age of the ATM : but for how long?, Banking Technology, November 1984, p 27

Banking Technology, 1985 : ATM security : the issues at stake, Banking Technology, June 1 1985, pp.43-45

Banking Technology, 1986a : Australian Banks Worry Over ATMs, Banking Technology, March 1986

Banking Technology, 1986b : Germany Reacts to ATM Fraud, Banking Technology, April 1986, p7

Banking Technology, 1987a : The Smart Card Comes of Age, Banking Technology, February 1987, pp.22-23

Banking Technology, 1987b : Australia's Telecom Plans EFTPOS Network, Banking Technology March 1987, pp.33-35

Banking Technology, 1987c : Taking the Lead with Networks, Banking Technology, July / August, 1987, pp.30-33

Banking World, 1985 : Security, Banking World, April 1985, pp.45-57

Beker, Henry and Piper, Fred, 1982 : Cipher Systems : The Protection of Communications, Wiley & Sons, New York

Beker, H.J, 1985 : Key management issues : a simple protocol for 'insecure' terminals, in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online, 1985

Bell Stephen, 1985 : Safety of EFTPOS 'mag stripes' questioned, National Business Review, March 18, pp.3-4

Bell, Stephen, 1986 : Finding a backup for the backup, National Business Review, August 29, p28

Benjamin, R.I, 1982 : Information Technology in the 1990's : A Long Range Planning Scenario, MIS Quarterly, Vol. 6, No. 2, pp.11-31

Bennet, R., 1976 : Economic Justification - A Look at ATMs, The Bankers Magazine, Spring 1976, pp.47-52

Bequai, August, 1981 : The Cashless Society : EFTS at the Crossroads, John Wiley & Sons, New York,

Bequai, August, 1983 : How To Prevent Computer Crime: A Guide for Managers, John Wiley & Sons, New York, 1983

Bequai, August, 1986 : Sources of EFT Liability, The Bankers Magazine, July-August, pp.81-83

Bequai, August, 1987 : Technocrimes, D.C. Heath & Company, United States of America

Berliet, D., 1985 : Costs and Benefits, in Smart Cards From France to the World, Editor Louis-Noel, July, pp.9-17

Beth, Thomas, 1985 : High speed implementations of public key crypto algorithms, in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Black, George, 1986 : Police say EFT is terrorist aim, Computer Weekly, May 1 1984, p1

Bosworth, Bruce, 1982 : Codes, Ciphers, and Computers, Hayden Book Company, Inc.Rochelle Park, New Jersey,

Boyle, William M., 1987 : Customer Safety at ATMs : How Big a Problem, Bank Administration, June 1987, pp.30-31

Braidwood D., 1987 : Implementation of IC Cards - Canada, Proceedings of Seminar on Microcircuit cards for the Financial Industry, March 1987, pp.41-44

British Computer Society Working Group on Testing, 1986 : Testing in Software Development, Cambridge University Press, Cambridge

Brown, Judy, 1987 : When It's More Than a Movie, Computer Weekly, May 1987, pp.30-31.

Brown, Ronald, 1983 : Electronic Banking 1, Post-News, Stoke-sub Hamdon, England,

Brown, Sarah and Brown, Ronald, 1986 : The Smart Card, Post-News, Stoke-sub Hamdon, England

Browne, Peter S., 1984 : How to Manage the Network Security Problem, Computer Security Journal, Summer 1984, pp.77-87

Bukowski, Robert., 1983 : ATM System Concerns for Senior Bank Managers, The Magazine of Bank Administration, February 1983, pp.28-32

Burford, Leigh, 1986 : Frauds - The Changing Pattern, The Australian Banker, October 1986 pp.210-215

Buurmeijer, F, 1984 : IBM's Data Security Strategy : Some Implementation Aspects, AFIPS Conference Proceedings, NCC Vol.46, pp.97-104

Caelli, William J., 1987 : Pressure grows for increased privacy in EFT transactions, Banker International, November 1987, pp.15-17

Caillon, Louis, 1985 : Development Prospects for Microcircuit Payment Cards in Smart Cards from France to the World, Editor Louis-Noel Joly, Lafferty

Cane, Alan, 1986 : Gearing Up to a Future Without CASH, The World of Banking, May/June 1986, pp.27-29

Catterall Tony, 1986 : Hackers crack Pin card, New Zealand Sunday Times, December 28, 1986, p17

Ceramalus, Nobilangelo, 1987 : Asset Aims to Please, Computerworld, September 7, 1987, p5

Chapin, W. and Soeder R., 1984 : ATM Security: A Summary of Controls, Magazine of Bank Administration, November 1984, pp.42-51

Chaum, David, 1985 : Security without identification : Transaction systems to make big brother obsolete, Communications of the ACM, Vol. 28 No. 10, pp.1030-1044

Church, Neil, 1987 : SWIFT II : cut-over postponed until 1988, Bankers International Magazine, March 1987, pp.12-13

Clark, James 1986 : Electronic Banking Security, Asiabanking, February 1986, pp.99-101

Clarke, Andrew, 1987 : Data security : banks adopt a more pragmatic approach, Banker International, September 1987, pp.7-12

Clayden, David, 1985 : Some methods of calculating the RSA potential, in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Clayton, Jenny, 1985 : Practical security for Value Added Network Services, System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Cline, Carol, 1986 : Daylight Overdrafts : The Fed Moves to Take Control, Banking Technology, March, 1986, pp.14-16

Cockcroft, John, 1984 : Chipping Away the Banks' Money, Banking World, October 1984, p. 27

Cohen, Fred 1987 : Computer Viruses : Theory and Experiments, Computers and Security 6 (1987), pp.22-23

Comer Michael, 1986 : Investigation of Banking Fraud, Computer Fraud and Security Bulletin, Vol. 8 No.12, pp.2-9

Computer Fraud and Security Bulletin, 1983a : Dead credit?, Computer Fraud and Security Bulletin, Vol. 6 No.1, p8

Computer Fraud and Security Bulletin, 1983b : Slavenburg arrests, Computer Fraud and Security Bulletin, Vol. 6 No.1, p9

Computer Fraud and Security Bulletin 1984a : Bank Telecommunications - Target For Fraud, Computer Fraud and Security Bulletin, Vol.6 No 6, p. 10

Computer Fraud and Security Bulletin 1984b : Wire Transfer and EFTS Frauds, Computer Fraud and Security Bulletin, Vol.6 No 5, pp.3-4

Computer Fraud and Security Bulletin, 1985a : Miscellaneous Bank Cases, Computer Fraud and Security Bulletin, Vol. 7 No. 4, p4

Computer Fraud and Security Bulletin, 1985b : Miscellaneous Hacking, Computer Fraud and Security Bulletin, Vol. 7 No.5, p3

Computer Fraud and Security Bulletin, 1985c : The Ultimate in Bad Luck, Computer Fraud and Security Bulletin Vol.7 No.7, p2

Computer Fraud and Security Bulletin, 1986 : Securing your networks, Computer Fraud and Security Bulletin Vol.8 No.8, pp.6-7

Computing Australia, 1986: Security in a Cashless Society, Computing Australia, 1986 : July 1986, p24

Cooper, James Arlin, 1984 : Computer-Security Technology, D.C Heath and Company, Lexington Mass.

Courtney Robert H. Jr., 1986 : Security Measures are inherently Undesirable, EDPACS, March 1986, pp.9-12

Cray, John 1987 : Automated Approach to System Security, CommUNIXations, September/ October 1987, pp.15-18

Crow, Walter, 1982 : Making the ATM More Secure, The Bankers Magazine, January - February 1982, pp.70 -74

Databank Systems Ltd., 1986 : Inter-bank Interactive Interchange Message Standards for Electronic Payment Systems, Databank Systems Ltd

Davies D.W., and Price W. L., 1984 : Security for Computer Networks, John Wiley and Sons

Davies, Donald W., 1983 : Applying the RSA Digital to Electronic Mail, IEEE, February 1983, pp.55-62

De Cotiis, Allen R. and Mel Ora, 1984 : Fulfilling the Promise of Direct Debit Point of Sale, The Bankers Magazine (U.S.), May-June 1984, pp.48-51

De Cotiis, Allen R, 1984 : The Business Plan for Home Banking, Federal Reserve Bank of Atlanta Economic Review, July-August 1984

Deignen, Terry, 1986: Transaction security for financial networks, Communications International, May 1986, pp.57-59.

De Mattia, R., 1985 : The Forces at Work in the Evolution of Payment Systems in the 1980s, Journal of Bank Research, Winter 1985, pp.211 -221

Denning, Dorothy E, 1983 : Protecting Public Keys and Signature Keys, IEEE, February 1983, pp.27-35

Denning, Dorothy E., 1982 : Cryptography and Data Security, Addison-Wesley Publishing Company Inc. Reading, Mass.

De Vallee, Patrice, 1987 : Computerisation : transforming NAR into a multipurpose operation, Bankers International Magazine, March 1987, pp.14-15

Dexter, A., 1986 : Two Into One Won't Go!, N.Z. Computer Scene, No. 8, 1986, pp.14-15

Dierkes H., 1987 : Results of Trials and Future Plans - Germany, Proceedings of Seminar on Microcircuit cards for the Financial Industry, March 1987, pp.33-40

Diffie W. and Hellman M., 1976 : New Directions in Cryptography, IEEE Trans. Information Theory, Vol. IT-22, No.6, November, pp.644-654

Dominion, 1986a : Software Error Costs $7.4m, Dominion, April 21, 1986, p14

Dominion, 1986b : British report on phantoms, Dominion, June 16, 1986, p18

Dominion, 1986c : Readers describe ATM trials, Dominion, June 23, 1986, p14

Dominion, 1986d: Machines botch up customer requests, Dominion, June 30, 1986, p20

Dominion, 1986e : Complaints file fills consumers' report, Dominion, June 30, 1986, p20

Dominion, 1987a : Power surge stops BNZ computers, Dominion, 12 February, 1987, p1

Dominion, 1987b : Technology Changes Open Loophole, Dominion, June 8, 1987, p23

Dominion, 1988 : Supersmart card goes on trial, Dominion, February 1, 1988, p23

Drucker, Peter F., 1964 : Managing for Results, Heinemann, London

Dvorkin, J., 1984 : What You Ought to Know About the Smart Card, Bankers Magazine (US), pp.44-49

EDPACS, 1985a : Computer Abuse, EDPACS, January, 1985, p14

EDPACS, 1985b : How Passwords are Cracked, EDPACS, September, 1985, pp.1-6

EDPACS, 1987 : Bank employee abuses authority, EDPACS, February 1987, p12

EDP Analyzer, 1986 : Information Security and Privacy, EDP Analyzer, Vol. 24 No.2, 1986, pp.1-11

Edwards, Darren, 1987 : Disaster Plans Can Ease Pain, Rydges, September 1987, pp.119-124

Ekebrink, Ivan, 1986 : Data Security in Terminalised System, Computers & Security 5 (1986), pp.325-327

Ellis H.Ray, 1983 : Protecting the ATM and its Customers, The Magazine of Bank Administration, December 1983, pp.42-52

England, Bevis, 1986 : The Hole in the Wall, Interface, October 1986, pp.20-23

Etheridge James, 1986 : Banking on a Safety Net, Datamation, November 1, 1986, pp.64-21 - 64-22

Evening Standard, 1986, December 22, 1986, p3

Everett, D., 1986 : Customer beware, Triple A, July 1986, pp.77-78

Fåk, Viivieke, 1987 : Crypto Management Made Manageable Demands on Crypto Equipment Design, Computer & Security 6 (1987), pp.36-40

Farquhar, Bill, 1986 : Computer crime 1986: an update of case history statistics, Computer Fraud and Security Bulletin, Vol. 9 No. 4, pp.1-9

Farr, Robert, 1975 : The Electronic Criminals, McGraw-Hill Book Company, New York

Faruqi, Nasreen Rehman, 1984 : Electronic Funds Transfer in the U.K. and Some Legal Aspects, Bank of Credit and Commerce International,,Economic Review, June 1984, pp.14-22

Fernandez, E.B., Summers, R.C., and Wood, C., 1981 : Database Security and Integrity, Addison-Wesley, U.S.A

Fisher, R.P, 1984 : Information Systems Security, Prentice Hall, Inc, New Jersey.

Fitch, Tony, 1987 : Amex enter battle with revolving credit, Banking Technology, May 1987, pp.27-28

Fitzgerald, Kevin, 1985: Pitfalls of Electronic Money Transactions, Pacific Computer Weekly, November 1 1985, p11

Friedman, Joel P., 1987 : The Changing World of Plastic Cards : A Revolution in Perspective, Journal of Retail Banking, Vol. 9 No. 1, pp.7-16

Gallant, Peter, 1985 : Electronic Treasury Management, Woodhead-Faulkner, Cambridge

Galloway Curtis C., 1987 : PIN-demonium, Risks-List : Risks-Forum, August 4, 1987, Vol.5, Issue 23

Glazer S., 1986 : Smart Cards, High Technology, July 1986, pp.34-43

Goeltz, Ted, 1986 : Why not DES?, Computers and Security 5, 1986, pp.24-27

Goldstone, Bruce, 1987 : Authentication Techniques, Presented at EDP Auditors Association Current Issues Seminar, Wellington, May 25 1987

Goldstone, Bruce, 1985 : Game Halls Linked To Hackers, The Dominion July 8, 1985, p 22

Good, Karlyn, 1983 : Home Banking Review 1983, Data Plus, Banta Book System USA

Gordon, John, 1985 : Implementation of the RSA, in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online,

Goslar A. R.,1986 : Smart Cards and Payment Systems Strategies, presented at EFTPOS & Home Services, 1986 International Conference, Edinburgh, November, Paper 8

Grimson, J.B. and Kugler, H.J (Ed.), 1985 : Computer Security : the practical issues in a troubled world, Elsevier Science Publishers, Dublin, Ireland

Group of Ten, 1982 : Security and Reliability In Electronic Systems For Payments, 2nd Revised Edition, Bank Administration Institute,

Guynes, Steve, 1986 : Security of Computer Software, ACM SIGSAC, Winter 1986 Vol. 4 No.1, pp.31-35

Hardwick, L.P., 1982 : Understanding the Debit Card, The Bankers Magazine (US), May-June 1982, pp.41-47

Harris Louis, 1985 : The Future of Technology in the Financial Services Industry, Coopers & Lybrand

Harper, Robert M.Jr., 1986 : Internal Control in Local Area Networks : an Accountant's Perspective, Computers & Security 5 (1986), pp.28-35

Hawk, Kathleen, 1987 : Plastic Warfare, United States Banker, June 1987, pp.40-43

Hayes, Jack, 1986 : Cutting Down the Risks, Better Business, August 1986, pp.72-75

Hayward, Richard G. and Kemp, Elizabeth A., 1987 : Information Systems and Security : A Strategic Perspective, Massey Computer Science Report 86/8, July 1987

Hayward, Richard G. and Kemp, Elizabeth A., 1987 : Manco: A Case Study in Computer Crime, Combating Computer Crime, Ed. Rae Weston, The Law Book Company Ltd. pp.52-72.

Heath, Sean, 1987 : EFTPOS At The Crossroads, Banking Technology, July / August 1987, pp.14-18

Hebden, C.T., 1985: Secure authentication in a local area network, in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Herman Joseph, 1987 : Bank Computers and flagging, Risks-List :Risks-Forum Digest 21 August 1987 Vol. 5, Issue 30

Highland, Harold Joseph, 1986 : The Demise of the DES, Computers & Security 5, 4 (1986) pp.3 -4

Highland, Harold Joseph, 1987 : The DES revisited - Part II, Computers & Security 6 (1987), pp.100-103

Hoffman, Lance J., 1977 : Modern Methods For Computer Security And Privacy, Prentice Hall Inc, New Jersey

Hoffman R., 1987 : $23-Million Computer SNAFU Adds to BofA's Troubles excerpted from Los Angeles Times Friday, July 24, 1987.Risks-List : Risks-Forum Digest 22 July 1987 Vol. 5, Issue 14

Hogg G., 1987 : Introduction, Description and Standards Issues, Proceedings of Seminar on Microcircuit cards for the Financial Industry, March 1987, pp.7-8

Hubbard, Richard, 1985 : EFT report dodges card protection, The Australian Financial Review, December 23, 1985, p1

Hutchins, David, 1985 : EFTPOS systems to be standardised?, Pacific Computing Weekly, April 26, 1985 p3

Intamic, 1987 : The Integrated Circuit Card, A "Tour D'Horizon", Intamic, February 1987

Interface, September 1986 : EFTPOS , Interface, pp.124-125

International Standards Organisation 7810, 1985 : Identification cards - Physical characteristics

International Standards Organisation 7811/1, 1985 : Identification cards - Recording Technique - Part 1: Embossing

International Standards Organisation 7811/1, 1985 : Identification cards - Recording technique -Part 5 : Location of read-write magnetic track - Track 3,

International Standards Organisation 7813, 1985 : Identification cards - Financial transaction cards

Jaben, Jan, 1986 : When Disaster Strikes, United States Banker, July 1986 pp.52-58

Jackson, Ivan F, 1986 : Corporate Information Management, Prentice-Hall, Englewood Cliffs, New Jersey.

Jacobs Geoff, 1984 : Steering a careful course through the security maze, Retail Banker 30 April, 1984, pp.5-8

James John.R., 1974 : Risk Management in Banking, American Bankers Association, Washington

Johnstone, Richard J, 1985 : Combatting fraudulent attacks on EFTPOS systems, in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Joly, Louis-Noel, 1985 : The Memory Card, in Smart Cards From France to the World, Editor Louis-Noel Joly, Lafferty

Jones, D., 1984 : Authorisation, Banking Technology, October 1984, pp.12-14

Jones, D., 1985 : EFTPOS finds its niche in petrol stations, Banking Technology, July 1985, pp.17-21

Jones, D., 1986 : The Smart Card Comes In From the Cold, Banking Technology, January 1986, pp.30-31

Journal of Cash Management, 1985: Editorial : Daylight Overdrafts, Fed Controls and the Corporate Cash Manager, Journal of Cash Management, May / June 1985, p10

Journal of Retail Banking 1987 : In Pursuit of More Advanced Card Technologies, Journal of Retail Banking, Vol.9 No. 1, pp.57- 60

Kahn, David, 1983 : Kahn on Codes, Macmillan Publishing Company, New York

Kaye Tony, 1987 : Westpac nodded and the system hiccupped, Australian Financial Review, June 9 1987, p72

Kelleher, Thomas F., 1985 : Countering Card Fraud, Banking Technology, November 1985, pp.12-15

Kemp E.A., 1985 : A comparative Study of Data Protection Features in Selected Database Management Systems, Project Report, Massey University, N.Z.

Kemp E.A., 1987 : Microcomputer Security - The EDP Auditor's Role, presented at EDPAC'87, Perth, March 6

Khanna S., 1985 : ATM Security : The Issues At Stake, Banking Technology, June 1985, pp.43-45

Klein, Mark M, 1987 : Data Security in Banks : Why, What and How, Bank Administration, May 1987, pp.72-74

Knowles, Terry, 1985 : An OSI architecture for secure communications, in System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Krauss, Leonard I. and MacGahan, Aileen, 1979 : Computer Fraud and Countermeasures, Prentice Hall, Inc, New Jersey

Kurzban, Stanley A., 1986 : Computing Systems Defences, Communications of the ACM, Winter 1986, Vol. 4 No.1, pp.1-27

Ladermann, Dan, 1986 : Toward the ever-evolving Open Systems Interconnect, Computer Design, July 1986, pp.113

Ladonceur L., 1987 : Results of Trials and Future Plans - Mastercard, Proceedings of Seminar on Microcircuit cards for the Financial Industry, March 1987, pp.17-20

Lane, V.P., 1985 : Security of Computer Based Information Systems, Macmillan Education Ltd, Hampshire and London

Langdale, J., 1985 : Electronic Funds Transfer and the Internationalisation of the Banking and Finance Industry, Geoform, Vol.16 No.1, pp.1-13

Latamore, G. Berton, 1987 : Do you know where your data's been ?, Computerworld, June 1, 1987 pp.75-81

Latamore, G. Berton. 1987 : Smart Cards Get Smarter, High Technology Business, September 1987, pp.35-37

Layer, R., 1985 : Network Security, in Smart Cards From France to the World, Editor Louis-Noel Joly, Lafferty

Le Clech, Phillipe G., 1987 : The rules that govern EFTPOS : New laws, and new uses for old ones, EFTPOS International Bulletin, May 1987, pp.10-13

Leclercq P. & Cormaille de Valbray, 1985 : How the French Legal System has Responded to the Smart Card, in Smart Cards From France to the World, Editor Louis-Noel Joly, Lafferty

Lenart, John, 1985 : Credit defamation - an emerging reality, Massey Journal of Asian and Pacific Business, October 1985

Linklater, Joan, 1986 : The Perils of New Directions, Triple A, March 1986, pp.54-55

Lipis, Allen H., Marshall Thomas R. and Linkes Jan H., 1985 : Electronic Banking, Wiley and Sons, New York,

List, William, 1986 : Accounting and Audit Implications of EFTPOS, presented at EFTPOS & Home Services, 1986 International Conference, Edinburgh, November, Paper 12

Lobb, Brenda, 1987 : Promotions, problems, EFTPOS pains, Interface, August 1987, pp.67-69

Louzoun, Michelle, 1987 : MasterCard Gives Credit to Information Technology, May 4 1987, Information Week, pp.60-62.

Lovition C.H., 1986 : Smart Card Moves Ahead In Europe, ABA Banking Journal, April 1986, pp.38-40

MacGibbon, John, 1987 : Which card? Which network?, Interface, June 1987

McGurk, J., 1985 : Emerging Payment Systems, The Australian Banker, April 1985, pp.66-69

McIvor, Robert, 1985 : Smart Cards, Scientific American, November 1985, pp.130-137

Mckenna, J., 1987 : Future Developments, Proceedings of Seminar on Microcircuit cards for the Financial Industry, March 1987, pp.45-48

MacLennan Catriona, 1987 : Techno-Crime, Accountants' Journal, Summary of the Proceedings of "Techno-Crimes " Conference, July 1987, pp.24-29

Mair, W.C., Wood, W.R. and Davis, K.W, 1978 : Computer Control and Audit, 11 A 363

Malecki A., 1986 : Pros and Cons of Smart Vs. Laser Vs Mag. Stripe Cards, presented at EFTPOS & Home Services, 1986 International Conference, Edinburgh, November, Paper 14

Marshall, Keith D. and Pylitt, Bernard L., 1987 : ATM Crime and Bank Liability, The Bankers Magazine, March-April 1987, pp.45-50

Martin, James, 1973 : Security, Accuracy, and Privacy in Computer Systems, Prentice-Hall, New Jersey

Martin, James, 1983 : An Information Systems Manifesto, Savant

Maurer, H., 1985 : Some remarks on videotex privacy and security, presented at Videotex International, Online Publications, Pinner UK

Mason, Rob, 1986 : Pinning down EFT, Australian Accountant, March 1986, pp.24-26

Meidan, A., 1984 : Marketing of bank credit cards, in Arthur Meidan, Bank Marketing Management, Macmillan, 1984

Mergle, David L., 1985 : Daylight Overdrafts and Payment System Risks, Federal reserve Bank of Richmond Economic Review, May-June 1985, pp.14-27

Meyer C.H.and Matyas S.M., 1982 : Cryptography : A New Dimension in Data Security, John Wiley and Sons, Brisbane

Michaud, A., 1985 : Experiments in France, in Smart Cards From France to the World, Editor Louis-Noel Joly, Lafferty

Middleton, R.A.J., 1986 : Security and reliability in banking, Computer Bulletin, March 1986, pp.32-34

Miller, Donald G., 1983 : Risk Assessment in Financial Institutions, Bank Administration Institute, Rolling Meadows, Illinois

Ministry of Consumer Affairs, 1987 : Code of practice to cover the issue and use of electronic funds transfer cards within New Zealand, Ministry of Consumer Affairs, Wellington

Moniez, J.C., 1986 : The Smart Card in France, Journal of Bank Research, Vol.16 No.4, pp.221-222

Myers, David, 1983 : With DP Skills On The Rise, Banks Concerned Over EFT Heists, Computerworld, December 5, 1983, p15

Naudts, John 1987 : How banking protects its technology, The Bankers Magazine, Sept.-Oct. 1987, pp.54-57

Nestman, Chadwick, Windsor, John, Hinsin, Mary, 1984 : Tutorial on Telecommunications and Security, Computers and Security 3 (1984), pp.215-224

Newman, S., 1984 : How to better use the S.W.I.F.T. Connection, Bankers Magazine, May - June 1984, pp.38-41

New Zealand Banker's Association, 1985 : EFT-POS : A Summary of the New Zealand trading banks' EFT-POS System, October 1985.

New Zealand Computer Scene, 1987 : The Changing Face of Financial Services, New Zealand Computer Scene No. 9, 1987, pp.12-13

Nilson Report, 1987 : Recent Examples of Violent Crime, The Nilson Report, January 1987, pp.4-6.

Norman, Adrian R.D, 1983 : Computer Insecurity, Chapman and Hall Ltd, London

Nutley, Mike, 1987 : Can the wrong hands be kept out of the till ? Datalink, June 1987, p8

NZPO, 1985 : A Proposal for a National Network Service for Electronic Funds Transfer at the Point of Sale (EFT / POS), NZPO, July 1985

Orkand Corporation, 1983 : ATM Networks...Strategic Issues, Research and Planning Department, Bank Marketing Association

Osterberg, R., 1984 : POS is on its way, Federal Reserve Bank of Atlanta Economic Review, July-August 1984, pp.32-35

Paget, W., 1985 : Australia : Towards a Financial Take-Off, Technology and the Future Bank Congress, Hong Kong, September 1985, pp.15-33

Parker, Donn B., 1976 : Crime By Computer, Charles Scribner's Sons, New York

Pehrson Judy 1986a : Phantoms haunt cash points, The Dominion, May 2 1986, p19

Pehrson Judy 1986b : Card proves expensive, The Dominion, June 16 1986, p18

Pehrson Judy 1986c: Funds transfer errors keep office busy, The Dominion, June 30, 1986, p20

Pehrson Judy, 1986d : Banks' EFT code too little, too late, The Dominion, 18 August, 1986, p23

Pehrson Judy 1987a : Pin money pirate, The Dominion, June 8, 1987, p22

Pehrson Judy 1987b : Wire delays lose money, The Dominion, August 24 1987, p23

Perkins, James H., 1984 : How to evaluate Risks in EFT Systems, The magazine of Bank Administration, February 1984, pp.56-62

Perry, William E., 1981 : Computer Control and Security, John Wiley & Sons, New York

Polis, R., 1985 : Protecting Card Payment Systems, Banking Technology, October 1985, pp.14 -16

Pomeroy, Lee, 1984 : Home Banking : Chemical Bank's Experience with Home Banking, Federal Reserve Bank of Atlanta Economic Review, July-August 1984.

POS News, 1984 : How much Security is Enough?, POS News, Newsletter of Retail Electronic Payments, October 1984, Vol. 1 No. 5, pp.1-3

Pritchard, J.A.T, 1978 : Computer Security : Risk Management in Action, The National Computer Centre Publications, Manchester

Pritchard, J.A.T, 1979 : Security in On-Line Systems, The National Computing Centre Publications, Manchester

Quantin, X., 1985 : Smart Card Security, in Smart Cards From France to the World, Editor Louis Noel Joly, Lafferty

Read, C., 1983 : Information Technology In Banking, Long Range Planning, Vol.16 No.4, pp.21-30

Rees, F., 1986 : Card Suppliers Prepare for Battle, Banking Technology, August 1986, p27

Rees, Frank, 1987 : Australia's Telecom Plans EFTPOS Network, Banking Technology, March 1987, pp.33-35

Retail Banker. 1984 : Hologram security could prove to be illusory, Retail Banker, 9 July 1984

Retail Banker, 1985 : Citicorp stung as fraud reveals flaws in Australian ATM networks, Retail Banker, July 1985, p 10

Revell, J., 1985 : Payment Systems over the Next Decade, Journal of Bank Research, Winter 1985, pp.200 -210

Revell, J., 1986 : Effects of New Technology on the Operations of Financial Institutions, World of Banking, September - October 1986, pp.26 - 30

Richards, R.M. and Yestingmeier J., 1986 : Risk Management - a Key to Security in Electronic Funds, Computers and Security 5 (1986) pp.135 -140

Risks-List, 1987 : Advertisements from the August issue of Computer Shopper, Risks-List : Risks-Forum Digest, July 20 1987, Vol. 5 Issue 13

Ritchie, Ian, 1987 : Audit Concerns for Users of Shared Transaction Switches, Presented at EDPAC 87, Perth, March 6

Rivest R.L., Shamir A., Adleman L., 1978 : A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM Vol. 21, No.2, February, pp120-126

Rockart, J.F, and Flannery, L.S, 1983 : The Management of End-user Computing, Communications of the ACM, Vol 26 No. 10, pp.776-784

Roff, G.A., 1985 : Guidelines for the protection of data on LANs, System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online

Royal, P., 1987 : Private Communication

Rutledge, Linda S. and Hoffman, Lance J., 1986 : A survey of Issues in Computer Network Security, Computers & Security 5 (1986) pp.296-308

Rydges, 1987 : A $ 10 000 Reminder, Rydges September 1987, pp.124-125

Sauls S. Walter and Towne Ann B., 1985 : How to Develop an Automated Kite Detection System, The Magazine of Bank Administration, August 1985, pp.34-36

Saunders, Michael, 1985 : Protecting Your Business Secrets, Nichols Publishing Company, New York.

Schnabel P., 1987 : Implementation of IC Cards -France, Proceedings of Seminar on Microcircuit cards for the Financial Industry, March 1987, p27-32

Seif, Ruth A, 1984 : Contingency Planning in the Banking Community, Computers and Security 3 1984, pp.29-34

Senzek, Alva, 1986 : After the Earthquake - How the Banks Fared, Banking Technology, June 1986, pp.36-38

Shamoon, S., 1986 : The Sharing of ATMs, Datamation, Vol.32 No. 6, pp.124-130.

Sigel, Efrem, 1986 : Is Home Banking For Real, Datamation, September 1986, pp.128-134

Smart Geoffrey and Evans Keith, 1986 : Building up the defences against the threat of felony, fraud or error, EFTPOS International Bulletin, May 1986, pp.11-13

Smith, Catherine, 1987 : Will EFTPOS really help the retailers improve service at the checkout desk?, EFTPOS International Bulletin, May 1987, pp.6-9

Smith, E.Everett, 1970 : Organizing for Bank Planning, The Bankers Magazine, Summer 1970, pp.19-27

Spiselman, David, 1984 : END POINTS : Cash Management Data Security, Journal of Cash Management, September / October 1984, pp.74-75

Stamper, David A, 1986 : Business Data Communications, The Benjamin / Cummings Publishing Company, California

Standards Association of Australia, 1985 : PIN Management and Security 2805.3

Standards Association of Australia, 1985 : Message Authentication AS 2805.4

Stanley, P., 1984 : Security, Rydges, August 1984, pp.86-89

Stanley, Thomas J, 1982 : Product Positioning for the Home Terminal, The Bankers Magazine (U.S.) May-June 1982

Stevens, F.J., 1984 : Risks in Large-Dollar Transfer Systems, Economic Review, Fall 1984, pp.2-27

Stone, B., 1984 : The revolution in Retail Payments : A Synthesis, Federal Reserve Bank of Atlanta Economic Review, July - August, 1984, pp.46-55

Streeter, Bill, 1982 : People, more than technology, are still key to EFT security, ABA Banking Journal, July 1982, pp.29-37

Svigals, J., 1987a : The Technology - A Review, Proceedings of Seminar on Microcircuit cards for the Financial Industry, March 1987, pp.9-16

Svigals, J. 1987b : Smart Cards - A Critical Decision Point., Journal of Retail Banking, Vol. 9 No. 1, pp.43-55

Svigals, J., 1987c : The smart card: Is it the wave of the future ? Retail Banker, 6 April 1987, pp.8-9

Tapper, Colin, 1983 : Computer Law, Longman House, Harlow

Thacker, K.H, 1983 :What is the business case for home banking? ABA Banking Journal, November 1983

Thomas, R., 1986 : Smart Cards ... Turning Our Money System On Its Head, Interface, February 1986, pp.19-21

Tompkins, Frederick G. & Rice, Russell 1986 : Integrating Security Activities into the Software Development Life Cycle and the Software Quality Assurance Process, Computers and Security 5 (1986), pp.218- 242

Trueman, Peter, 1986 : Security for distributed systems, Data Processing, Vol.28 No.4, May 1986, pp.187-190

Trusteebanks, 1986 : Neutral Network, N.Z. Computer Scene, No. 8, 1986, pp.7-8

Tucker, G., 1986 : A Legal Implication For Automated Teller Machines, The Australian Banker, June, pp.119-120

Tunstall, J., 1985 : "Smart Cards-their applications & security features" System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online, pp.1-8

Tunstall, J., 1987 : Development of Standards, Proceedings of Seminar on Microcircuit cards for the Financial Industry, March 1987

Tutt Nigel, 1987 : The Smart Card Comes Of Age, Banking Technology, February, pp.24-25

Tyree, Alan, 1985 : EFT / POS Etc..., Interface, February 1985, pp.17- 23

U.S. Department of the Treasury, 1985 : Criteria for Testing, Evaluating, and Certifying Message Authentication Devices for Federal E.F.T. Use

Van Duyn, Julia, 1985 : Security in Computer Installations, Data Processing, Vol. 27 No. 6, July/August 1985, pp.19-22

Wagner, Charles R., 1979 : The CPA and Computer Fraud, D.C.Heath and Company, USA

Webster, G.J.L, 1985. : Security Issues in Home Banking, System security the technical challenge, Proceedings of the international conference held in London, October 1985, Online Publications, 1985, pp.31-39

Weston, Rae, 1987 : Preventing Credit Card Crime, in Combating Commercial Crime, The Book Company Limited, Sydney, 1987

Wightman, David, 1986 : The Different Approach in USA to EFTPOS, EFTPOS & Home Services, 1986 International Conference, Edinburgh, November, Paper 7

Williamson, J.M., 1986 : APACS - A Revolution in UK Payment Systems, World of Banking, September - October 1986, pp.12 -16

Williamstad, Robert B, 1984 : A Home Banking Case Study, The Bankers Magazine (U.S.), November-December 1984

Winters, Chester M., 1985 : Auditing the Technical Support Function, The EDP Audit Control and Security Newsletter, February 1985, pp.1-7

Winters, Chester M., 1986 : ATM Control, Audit and Security, Management Advisory Publications, Wellesley Hill, Mass.

Wong, K.K, 1977 : Computer Security Risk Analysis and Control : a guide for the DP manager, National Computing Centre Publications, Manchester, 1977

Wong, Ken, 1986 : The Hackers and Computer Crime Against Financial Institutions, EDPACS November 1986 pp.1-7

Wong, Ken, 1987 : Data Security - Watch Out For The New Computer Criminals, Computer Fraud and Security Bulletin, Vol 9 No.6, pp.7 - 13

Wong, Ken and Farquhar Bill, 1987 : Computer disaster statistics 1987, Computer Fraud and Security Bulletin Vol 9 No. 8, pp.1-9

World of Banking, 1986 : Emerging Trends in ATM Developments, The World of Banking, January/February 1986, pp.17-19

Zimmer Linda Fenner, 1986 : ATM Products and Service, The World of Banking, July-August 1986, pp.22-29

Zimmer Linda Fenner, 1987 : ATMs : An Industry Status Report, Bank Administration, May 1987, pp.30-39