Encryption Key Management in Wireless Ad Hoc Networks

A thesis presented in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy in Computer Science

at Massey University, Auckland, New Zealand

Alastair Jon Nisbet

2010

Abstract

Communication is an essential part of everyday life, both as a social interaction and as a means of collaboration to achieve goals. Networking technologies including the Internet have provided the ability to communicate over distances quickly and effectively, yet the constraints of having to be at a computer connected to a network access point restricts the use of such devices. Wireless technology has effectively released the users to roam more freely whilst achieving communication and collaboration, and with worldwide programs designed to increase laptop usage amongst children in developing countries to almost 100%, an explosive growth in wireless networking is expected. However, wireless networks are seen as relatively easy targets for determined attackers. Security of the network is provided by encrypting the data when exchanging messages and encryption key management is therefore vital to ensure privacy of messages and robustness against disruption.

This research describes the development and testing through simulation of a new encryption key management protocol called SKYE (Secure Key deploYment & Exchange) that provides reasonably secure and robust encryption key management for a mobile ad hoc network. Threshold cryptography is used to provide a robust Certificate Authority providing certificate services to the network members using Public Key Infrastructure. The protocol is designed to be used in an environment where communications must be deployed quickly without any prior planning or prior knowledge of the size or numbers of the potential members. Such uses may be many and varied and may include military, education or disaster recovery where victims can use the protocol to quickly form ad hoc networks where other communication infrastructure has failed. Many previous protocols were examined and several key

features of these schemes were incorporated into this protocol along with other unique features. These included the extensive tunability of the protocol allowing such features as increasing the number of servers that must collaborate to provide services and the trust level that must exist along a certificate chain before a request for a certificate will be accepted by a server. The locations of the servers were carefully selected so that as these parameters were altered to increase security, performance remained high. For example, when two servers were required for certificate issuance, a certificate request would succeed 92% of the time. By doubling the servers required and therefore considerably increasing resilience against attack of the certificate authority, this figure dropped only moderately to 78%. The placement of the servers proved to be a critical parameter and extensive experiments were run to identify the best placements for servers with the various parameters chosen.

Simulations show that the protocol performs effectively in a developing and constantly changing network where nodes may join and leave the network frequently and where many of the members may be mobile. The many tunable parameters of the protocol ensure that it is useful in a variety of applications and has unique features making it effective and efficient in a highly dynamic network environment.

Acknowledgements

I would like to thank the many people who have provided encouragement and advice during the time that this research was undertaken. Thanks to my supervisor Dr Mohammed Rashid who provided enthusiastic supervision that ensured the research continued its course towards completion. His knowledge, advice and encouragement during difficult times were a source of inspiration.

Thanks also to my co-supervisor Dr Fakhrul Alam who provided advice and support with the technical aspects of this research and to the School of Engineering and Applied Science at Massey University that provided resources and facilities required to complete the research.

I am very grateful to my previous supervisor Dr Ellen Rose who provided a wealth of knowledge and experience to ensure the research took an unfaltering path during her time as my supervisor.

The completion of this thesis is a testament to the unwavering support of my wife, Ruth who provided many years of support whilst I undertook a lifelong ambition. To her I will be eternally grateful.

This thesis is dedicated to my wife and our two wonderful little children, Thomas and Skye who have suffered the trials and tribulations of Doctoral research at times as much as me. Thank you to my wonderful family.

Table of Contents

List of Figures

List of Tables

List of Publications

Nisbet, A. J. *Wireless Networks in Education – A New Zealand Perspective*. Proceedings of the IIMS Postgraduate Conference 2004, Massey University, Auckland, 2004.

Nisbet, A.J. *An Improved Encryption Key Management System for IEEE 802.16 Mesh Mode Security Using Simulation.* Proceedings of the Fifth New Zealand Computer Science Research Student Conference, Waikato University, Hamilton, 2007.

Nisbet, A.J. Rashid M.A., *A Scalable & Tunable Encryption Key Management System for Mobile Ad Hoc Networks.* Proceedings of the 2009 International Conference on Wireless Networks, Las Vegas, USA, 2009.

Nisbet, A.J, Rashid M.A, Alam, F. *The Quest for Optimum Server Location Selection in Mobile Ad Hoc Networks Utilising Threshold Cryptography.* Proceedings of the 7th International Conference on International Technology: New Generations. Las Vegas, USA, 2010.

Nisbet, A.J, Rashid M.A. *Performance Evaluation of Secure Key Deployment and Exchange Protocol for MANETs.* Accepted for International Journal of Secure Software Engineering (IJSSE), 2010.

Abbreviations and Acronyms

AAA	Authentication Authorisation and Accounting
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
AS	Access Server
BPSK	Binary Phase Shift Keying
BSS	Basic Service Set
CA	Certificate Authority
CCK	Complimentary Code Keying
CCM	Clear Channel Assessment under MAC
CPU	Central Processing Unit
CRC	Cyclic Redundancy Checksum
CSMA/CA	Carrier Sense Multiple Access / Collision Avoidance
DBPSK	Differential Binary Phase Shift Keying
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DQPSK	Differential Quadrature Phase Shift Keying
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol Over LAN
ETSI	European Telecommunications Standards Institute
ERP	Extended Rate PHY
IBSS	Independent Basic Service Set
IC	Integrity Check
ICV	Integrity Check Value
ID	Identity
IEEE	Institute of Electronics and Electrical Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
IV	Initialisation Vector

FCC	Federal Communications Commission
FH	Frequency Hopping
GHz	Gigahertz
ISM	Industrial Scientific and Medical
KDC	Key Distribution Centre
KGS	Key Generation Server
KM	Key Management
KMS	Key Management Service
L2F	Layer 2 Forwarding
LAN	Local Area Network
MAC	Media Access Control
MANET	Mobile Ad Hoc Network
Mbps	Mega bits per second
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MPDU	MAC Packet Data Unit
MSDU	MAC Service Data Unit
MTM	Man in The Middle
NAS	Network Access Server
OFDM	Orthogonal Frequency Division Multiplexing
PBCC	Packet Binary Convolutional Coding
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PHY	Physical Layer
PKI	Public Key Infrastructure
PMK	Pre-shared Master Key
PPTP	Point To Point Tunnelling protocol
PRNG	Pseudo Random Number Generator
PSK	Pre-Shared Key
PTK	Pre-shared Temporal Key
PTMP	Point to Multi Point
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying

RADIUS	Remote Access Dial In User Service
RFMon	Radio Frequency Monitor Mode
RTS/CTS	Request to Send / Clear to Send
STA	Station
TGT	Ticket Granting Ticket
TKIP	Temporal Key Integrity Protocol
TTP	Trusted Third Party
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WPA	WiFi Protected Access
XOR	Exclusive Or