Copyright is owned by the Author of the thesis. Permission is given for a copy to be downloaded by an individual for the purpose of research and private study only. The thesis may not be reproduced elsewhere without the permission of the Author.

Ontological Lockdown Assessment

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

Master of Science

in

Information Technology

at Massey University, Palmerston North, New Zealand

Aaron Steele

2008

Abstract

In order to keep shared access computers secure and stable system administrators resort to locking down the computing environment in order to prevent intentional and unintentional damage by users. Skilled attackers are often able to break out of locked down computing environments and intentionally misuse shared access computers. This misuse has resulted in cases of mass identity theft and fraud, some of which have had an estimated cost ranging in millions.

In order to determine if it is possible to break out of locked down computing environments an assessment method is required. Although a number of vulnerability assessment techniques exist, none of the existing techniques are sufficient for assessing locked down shared access computers. This is due to the existing techniques focusing on traditional, application specific, software vulnerabilities. Break out path vulnerabilities (which are exploited by attackers in order to break out of locked down environments) differ substantially from traditional vulnerabilities, and as a consequence are not easily discovered using existing techniques.

Ontologies can be thought of as a modelling technique that can be used to capture expert knowledge about a domain of interest. The method for discovering break out paths in locked down computers can be considered expert knowledge in the domain of shared access computer security. This research proposes an ontology based assessment process for discovering break out path vulnerabilities in locked down shared access computers. The proposed approach is called the ontological lockdown assessment process. The ontological lockdown assessment process is implemented against a real world system and successfully identifies numerous break out path vulnerabilities.

Acknowledgements

Firstly, I thank Jesus. Also, my lovely wife Sina, my supervisors: Sven Hartmann and Sebastian Link. Thanks also go to Stephen Marsland, Elizabeth Kemp, and Patrick Rhyhart, my Church and all the people therein.

Last of all I thank everyone else who helped me during the course of this project.

This thesis is dedicated to one of the finest graduates of Ngaumu University, my granddad, Bob Coulson.

Publications

A publication related to this research is:

Steele, A. (2008). Ontological Vulnerability Assessment. *Proceedings of the International Workshop on Web Information Systems Engineering for Electronic Businesses and Governments (E-BAG 2008)*. S. Hartmann et al. (Eds): WISE 2008, LNCS 5176, pp. 24-35, 2008. © Springer-Verlag Berlin Heidelberg 2008

Table of Contents

Abstract I
Acknowledgements II
Publications III
Table of Contents IV
List of Figures VII
List of Tables VIII
1 Introduction 1
1.1 Research Objectives 1
1.2 Thesis Structure 2
2 The Lockdown Problem 4
2.1 Shared Access Computers 4
2.2 Unique Security Issues 5
2.2.1 Perceived Value 5
2.2.2 Usability, Security and Cost Trade Off 7
2.2.3 Insider Threat 8
2.2.4 User Information 9
2.2.5 Dormant Technology 9
2.3 Potential Attacks 10
2.3.1 History 11
2.3.2 Key Logging 11
2.3.3 Shares 13
2.3.4 Sniffing 13
2.3.5 Scanning 14
2.3.6 Denial of Service and Vandalism 15
2.4 Problem Summary 15
2.4.1 Locking down 16
2.4.2 Tools and Techniques 19
2.4.3 Problem Statement 19
3 Existing Vulnerability Assessment Techniques 21
3.1 Vulnerability Scanners 21

3.1.1 Nessus 21
3.1.2 GFI LANguard 23
3.1.3 Other Vulnerability Scanners 24
3.2 Vulnerability Assessment Procedures 25
3.2.1 NIST Risk Management Guide 25
3.2.2 FRAP 28
3.2.3 VAM 30
3.2.4 Pfleeger & Pfleeger 32
3.3 Summary of Existing Techniques 34
4 An Ontological Solution 36
4.1 Ontologies 36
4.1.1 Definition 36
4.1.2 Features 38
4.2 Ontologies in Security 39
4.2.1 NRL Security Ontology 40
4.2.2 An Ontology for Network Security Attacks 40
4.2.3 Security Ontology as a Methodical Tool 41
4.2.4 Ontologies for Security Planning 42
4.2.5 Ontologies for Security Critical Software Development 42
4.2.6 Ontologies for Security Management 43
4.2.7 Summary of Ontologies in Security 46
4.3 Proposed Ontological Solution 47
5 Lockdown Assessment Ontology 48
5.1 Breaking Out 48
5.1.1 Example One 48
5.1.2 Example Two 49
5.1.3 Example Three 50
5.1.4 Example Four 51
5.2 The Underlying Principles 52
5.2.1 Inputs 53
5.2.2 Processes and Outputs 54
5.3 The Ontology 55
5.4 Ontological Lockdown Assessment 57
5.4.1 Phase 1: Define the Broken State 58

5.4.2 Phase 2: Identify the Initial Assets 59
5.4.3 Phase 3: Build Access Paths 60
5.4.4 Phase 4: Compilation and Analysis 61
6 Case Study 63
6.1 System Characteristics 63
6.2 Ontological Lockdown Assessment 64
6.2.1 Phase 1: Define the Broken State 64
6.2.2 Phase 2: Identify the Initial Assets 64
6.2.3 Phase 3: Build Access Paths 65
6.2.4 Phase 4: Compilation and Analysis 73
6.3 Comparative Results 80
6.3.1 Vulnerability Scanner 80
6.3.2 Online Vulnerability Databases 86
6.4 Case Study Summary 88
7 Conclusion 89
7.1 Review 89
7.2 Future 90
7.3 Limitations 91
7.4 Discussion 92
References 94

List of Figures

Figure 1. Usability, security and cost trade off triangle for computer security 7
Figure 2. Function sets of a perfectly locked down shared access computer 17
Figure 3. Function sets of an imperfectly locked down shared access computer 18
Figure 4. FRAP Brainstorming Guide [55] (p. 78) 29
Figure 5. The VAM Vulnerability Matrix [20] (p. 27) 31
Figure 6. Assets and Security Properties [57] (p. 529) 33
Figure 7. Asset, threat, countermeasure ontology model 45
Figure 8. Generic Microsoft Narrator dialog box 50
Figure 9. The basic IPO model 52
Figure 10. Ontology of the break out process 55
Figure 11. Ontological Asset to Access Point path 57
Figure 12. Screen Control Panel access paths in graph format 74
Figure 13. Interconnect access path graph 75
Figure 14. Keyboard port and Mouse port access paths in graph format 76

List of Tables

Table 1. Asset to security attribute relationship table [65] 44
Table 2. Improved asset to security attribute relationship table 45
Table 3. Screen Control Panel vulnerability impact ratings 77
Table 4. Keyboard and Mouse port vulnerability impact ratings 77
Table 5. Interconnected break out path vulnerability impact ratings..... 79
Table 6. Comparative Nessus vulnerability scan results..... 86