Vulnerability Analysis and Defense for the Internet

Advances in Information Security

Sushil Jajodia
Consulting Editor
Center for Secure Information Systems
George Mason University
Fairfax, VA 22030-4444
email: jajodia@gmu.edu

The goals of the Springer International Series on ADVANCES IN INFORMATION SECURITY are, one, to establish the state of the art of, and set the course for future research in information security and, two, to serve as a central reference source for advanced and timely topics in information security research and development. The scope of this series includes all aspects of computer and network security and related areas such as fault tolerance and software assurance.

ADVANCES IN INFORMATION SECURITY aims to publish thorough and cohesive overviews of specific topics in information security, as well as works that are larger in scope or that contain more detailed background information than can be accommodated in shorter survey articles. The series also serves as a forum for topics that may not have reached a level of maturity to warrant a comprehensive textbook treatment.

Researchers, as well as developers, are encouraged to contact Professor Sushil Jajodia with ideas for books under this series.

Additional titles in the series:

BOTNET DETECTION: Countering the Largest Security *Threat* edited by Wenke Lee, Cliff Wang and David Dagon; ISBN: 978-0-387-68766-7

PRIVACY-RESPECTING INTRUSION DETECTION by Ulrich Flegel; ISBN: 978-0-387-68254-9

SYNCHRONIZING INTERNET PROTOCOL SECURITY (SIPSec) by Charles A. Shoniregun; ISBN: 978-0-387-32724-2

SECURE DATA MANAGEMENT IN DECENTRALIZED SYSTEMS edited by Ting Yu and Sushil Jajodia; ISBN: 978-0-387-27694-6

NETWORK SECURITY POLICIES AND PROCEDURES by Douglas W. Frye; ISBN: 0-387-30937-3

DATA WAREHOUSING AND DATA MINING TECHNIQUES FOR CYBER SECURITY by Anoop Singhal; ISBN: 978-0-387-26409-7

SECURE LOCALIZATION AND TIME SYNCHRONIZATION FOR WIRELESS SENSOR AND AD HOC NETWORKS edited by Radha Poovendran, Cliff Wang, and Sumit Roy; ISBN: 0-387-32721-5

PRESERVING PRIVACY IN ON-LINE ANALYTICAL PROCESSING (OLAP) by Lingyu Wang, Sushil Jajodia and Duminda Wijesekera; ISBN: 978-0-387-46273-8

SECURITY FOR WIRELESS SENSOR NETWORKS by Donggang Liu and Peng Ning; ISBN: 978-0-387-32723-5

MALWARE DETECTION edited by Somesh Jha, Cliff Wang, Mihai Christodorescu, Dawn Song, and Douglas Maughan; ISBN: 978-0-387-32720-4

ELECTRONIC POSTAGE SYSTEMS: Technology, Security, Economics by Gerrit Bleumer; ISBN: 978-0-387-29313-2

Additional information about this series can be obtained from http://www.springer.com

Vulnerability Analysis and Defense for the Internet

by

Abhishek Singh (Editor)
SafeNet Infotech Pvt.Ltd.
Noida, India

Baibhav Singh
SafeNet Infotech Pvt.Ltd.
Noida, India
and
Hirosh Joseph
Third Brigade
Ottawa, Ontario,Canada

Springer

Editor
Abhishek Singh
SafeNet Infotech Pvt. Ltd.
Logix Technopark
Sector-127 Taj Express Way
Noida – 201301, UP, India

with contributions by

Baibhav Singh
SafeNet Infotech Pvt. Ltd.
Logix Technopark
Sector-127 Taj Express Way
Noida – 201301, UP, India

Hirosh Joseph
Third Brigade
40 Hines Rd.
Ottawa, K2K 2M5Ontario,
Canada

Series Editor
Sushil Jajodia
George Mason University
Center for Secure Information Systems
Research I, Suite 417
Fairfax VA 22030-4444
jajodia@gmu.edu

ISBN: 978-0-387-74389-9 e-ISBN: 978-0-387-74390-5

Library of Congress Control Number: 2007941398

Cover illustration:

Printed on acid-free paper

9 8 7 6 5 4 3 2 1

springer.com

Table of Contents

1.0 Wireless Security 1
1.1 Introduction 1
1.2 Wired Equivalent Privacy protocol 1
1.2.1 Analysis of WEP flaws 3
1.2.2 Key Stream Reuse 3
1.2.3 Message Modification 3
1.2.4 Message Injection 4
1.2.5 Authentication Spoofing 6
1.2.6 IP Redirection 7
1.2.7 Wireless Frame Generation 7
1.2.7.1 AirJack 8
1.2.7.2 Wavesec 9
1.2.7.3 Libwlan 9
1.2.7.4 FakeAP 9
1.2.7.5 Wnet 10
1.2.7.7 Scapy 10
1.2.8 Encryption Cracking Tools 11
1.2.8.1 Wepcrack 12
1.2.8.2 Dweputils 12
1.2.8.3 Wep_tools 13
1.2.8.4 Wep Attack 14
1.2.9 Retrieving the WEP keys from Client Host 14
1.2.10 Traffic Inection Tools 15
1.2.11 802.1x Cracking Tools 16
1.2.11.1 Asleap-imp and Leap 16
1.2.12 Wireless DoS Attacks 17
1.2.12.1 Physical Layer Attack or Jamming 17
1.2.12.1.1 Signal Strength 18
1.2.12.1.2 Carrier Sensing Time 18
1.2.12.1.3 Packet Delivery Ratio 19
1.2.12.1.4 Signal Strength Consistency check 20
1.2.12.2 Spoofed Dessociation and Deauthentication Frames 20
1.2.12.3 Spoofed Malformed Authentication Frames 21
1.2.12.4 Flooding the Access Point Association and Authentication Buffer 21
1.2.12.5 Frame Deletion Attack 22
1.2.12.6 DoS attack dependent upon specific Wireless Setting 22
1.2.13 Attack against the 802.11i implementations 23
1.2.13.1 Authentication Mechanism Attacks 23
1.3 Prevention and Modifications 25
1.3.1 TKIP: temporal Key Integrity Protocol 27

1.3.1.1 TKIP Implementation 27
1.3.1.1.1 Message Integrity 28
1.3.1.1.2 Initialization Vector 29
1.3.1.1.3 Prevention against the FMS Attack 31
1.3.1.1.4 Per Packet key Mixing 31
1.3.1.1.5 Implementation Details of TKIP 32
1.3.1.1.6 Details of Per Packet Key mixing 33
1.3.1.2 Attack on TKIP 38
1.3.2 AES – CCMP 39
1.3.2.1 CCMP Header 40
1.3.2.2 Implementation 40
1.3.2.2.1 Encryption Process in MPDU 41
1.3.2.2.2 Decrypting MPDU 42
1.4 Prevention Method using Detection Devices 43
1.5 Conclusion 46

2.0 Vulnerability Analysis for Mail Protocols 47
2.1 Introduction 47
2.2 Format String Specifiers 48
2.2.1 Format String Vulnerability 49
2.2.1.1 Format String Denial of Service Attack 49
2.2.1.2 Format String Vulnerability Reading Attack 50
2.2.1.3 Format String Vulnerability Writing Attack 51
2.2.1.4 Preventive Measures for Format String vulnerability 53
2.3 Buffer Overflow Attack 54
2.3.1 Buffer Overflow Prevention 56
2.4 Directory Traversal Attacks 60
2.4.1 Remote Detection 62
2.5 False Positive in Remote Detection for Mail Traffic 63
2.5.1 False Positive in case of SMTP Traffic 64
2.5.2 False Positive in case of IMAP Traffic 67
2.6 Conclusion 70

3.0 Vulnerability Analysis for FTP and TFTP 71
3.1 Introduction 71
3.1.1 Buffer Overflow in FTP 72
3.1.2 Directory Traversal Attack in FTP 73
3.2 TFTP Vulnerability Analysis 74
3.2.1 Vulnerability Analysis 75
3.3 Conclusion 77

4.0 Vulnerability Analysis for HTTP 79
4.1 Introduction 79
4.2 XSS Attack 79
4.2.1 Prevention against Cross Site Scripting Attacks 82
4.2.1.1 Vulnerability Protection 82

4.3 SQL Injection Attacks 88
4.3.1 SQL Injection Case Study 90
4.3.2 Preventive Measures 93
4.3.2.1 Remote Detection 93
4.3.2.2 SQL injection in Oracle Data base 94
4.3.2.2.1 Stored Procedures 94
4.3.2.2.2 Remote Detection for Oracle Database 96
4.3.3 Other Preventive Measures 100
4.3.3.1 Preventive Measures by developers 101
4.4 MS DoS Device Name Vulnerability 101
4.4.1 Prevention from DoS Device Name Vulnerability 103
4.5 False Positive in HTTP 103
4.6 Evasion of HTTP Signatures 105
4.7 Conclusion 109

5.0 Vulnerability Analysis for DNS and DHCP 111
5.1 Introduction of DNS Protocol 111
5.1.1 Vulnerabilities in a DNS Protocol 113
5.1.1.1 DNS Cache Poisoning 113
5.1.1.2 Redirection Attack 116
5.1.1.3 Buffer Overflow Vulnerability 116
5.1.1.4 DNS Man in the Middle Attack or DNS Hijacking 116
5.1.1.5 DNS Amplification Attack 117
5.1.2 False Positives in a DNS Protocol 118
5.2 Introduction of DHCP 120
5.2.1 Vulnerabilities in DHCP 120
5.2.1.1 Client Masquerading 120
5.2.1.2 Flooding 121
5.2.1.3 Client Misconfiguration 121
5.2.1.4 Theft of Service 121
5.2.1.5 Packet Altercation 121
5.2.1.6 Key Exposure 121
5.2.1.7 Key Distribution 122
5.2.1.8 Protocol Agreement Issues 122
5.2.2 False Positive in DHCP 122
5.3 Conclusion 124

6.0 Vulnerability Analysis for LDAP and SNMP 125
6.1 Introduction 125
6.2 ASN and BER Encoding 125
6.3 BER implementation for LDAP 127
6.3.1 Threat Analysis for Directory Services 129
6.4 SNMP 131
6.4.1 Vulnerability Analysis for SNMP 134
6.5 Conclusion 134

7.0 Vulnerability Analysis for RPC 135
7.1 Introduction..... 135
7.2 RPC Message Protocol 136
7.3 NDR Format 136
7.4 Port Mapper 152
7.5 False Positive for SMB RPC Protocol 153
7.6 Evasion in RPC..... 157
7.6.1 Multiple Binding UUID 157
7.6.2 Fragment Data across many Requests 158
7.6.3 Bind to one UUID then alter Context 159
7.6.4 Prepend an ObjectID 161
7.6.5 Bind with an authentication field 161
7.6.6 One packet UDP function call 162
7.6.7 Endianess Selection..... 162
7.6.8 Chaining SMB commands 163
7.6.9 Out of order chaining 164
7.6.10 Chaining with random data in between commands..... 165
7.6.11 Unicode and non-Unicode evasion 165
7.6.12 SMB CreateAndX Path Names..... 166
7.7 Conclusion 167

8.0 Malware 169
8.1 Introduction..... 169
8.2 Malware Naming Convention 169
8.2.1 Worms 170
8.2.2 Trojans 171
8.2.3 Spyware & Adware 172
8.3 Malware Threat Analysis 173
8.3.1 Creating controlled Environment..... 173
8.3.1.1 Confinement with the Hard Virtual Machines 173
8.3.1.2 Confinement with the Soft Virtual Machines..... 174
8.3.1.3 Confinement with Jails and Chroot 176
8.3.1.4 Confinement with System call Sensors 177
8.3.1.5 Confinement with System call Spoofing 178
8.3.2 Behavioral Analysis 178
8.3.3 Code Analysis..... 180
8.4 Root Kits..... 181
8.4.1 User and Kernel Mode Communication 182
8.4.2 I/O Request Packets (IRP) 183
8.4.3 Interrupt Descriptor Table..... 189
8.4.4 Service Descriptor Table..... 190
8.4.5 Direct Kernel Object Manipulation 194
8.4.6 Detection of Rootkits 196
8.5 Spyware 197
8.5.1 Methods of Spyware installation and propagation 199
8.5.1.1 Drive- By- Downloads..... 199
8.5.1.2 Bundling..... 201

8.5.1.3 From Other Spyware 203
8.5.1.4 Security Holes 203
8.5.2 Vulnerability Analysis 203
8.5.2.1 Iframe Exploit 203
8.5.2.2 IE .chm File processing Vulnerability 204
8.5.2.3 Internet Code Download Link 205
8.5.3 Anti Spyware Signature Development 207
8.5.3.1 Vulnerability Signature 207
8.5.3.2 CLSID Data base 208
8.5.3.3 Spyware Specific Signature 208
8.5.3.4 Information Stealing 210
8.5.3.5 Preventing Information from being sent as emails 210
8.6 Conclusion 210

9.0 Reverse Engineering 213
9.1 Introduction 213
9.2 Anti Reversing Technique 213
9.2.1 Anti Disassembly 214
9.2.1.1 Linear Sweep Disassembler 214
9.2.1.2 Recursive Traversal Disassembler 216
9.2.1.3 Evasion Technique for Disasembler 217
9.2.2 Self-Modifying Code 220
9.2.3 Virtual Machine Obfuscation 224
9.3 Anti Debugging Technique 225
9.3.1 Break Points 227
9.3.1.1 Software break point 227
9.3.1.2 Hardware break point 228
9.3.1.3 Detection of Breakpoint 229
9.4 Virtual Machine Detection 229
9.4.1 Checking finger print 230
9.4.2 Checking system tables 230
9.4.3 Checking processor instruction set 231
9.5 Unpacking 232
9.5.1 Manual unpacking of malware 233
9.5.1.1 Finding an original entry point of an executable 233
9.5.1.2 Taking memory Dump 238
9.5.1.3 Import Table Reconstruction 241
9.5.1.4 Import redirection and code emulation 246
9.6 Conclusion 250

Index 253

Preface

Vulnerability Analysis is a process that defines, identifies, and classifies the vulnerabilities in a computer network or an application. Vulnerability in a network or application can in turn be used to launch various attacks like cross-site scripting attacks, SQL injection attacks, format string attacks, buffer overflows, DNS amplification attacks etc.

Although these attacks are not new and are well known, the number of vulnerabilities disclosed to the public jumped nearly 5 percent during the first six months of 2007. This accounts to be the fourth year report, which shows the raise in vulnerability (see the news link on security focus http://www.securityfocus.com/brief/614). In January 2007, a vulnerable network resulted in a theft of 45.6 million credit card numbers in TJX companies due to unauthorized intrusion.

A good protocol analysis and effective signature writing is one of the effective method to prevent vulnerability and minimize the chances of intrusion in the network. However, protocol analysis poses two challenges namely false positive and evasion. If the signature to prevent the vulnerability is not written properly, it will result in dropping of a valid traffic thereby resulting in false positive. An effective signature should also consider the chances of evasion; otherwise a malicious attacker can use the variant of exploit and evade the protection provided by the IDS/IPS.

This book discusses the structure of protocol and provides a thorough understanding of the structure, which is crucial in writing signatures. It also discusses the pseudo code of algorithms, which can be used to reduce false positives. The chapters in this book are prepared with an assumption that the reader is familiar with the protocols and RFC of various protocols. The reader should also have knowledge on using basic tools like ethereal.

Chapter 1 deals with wireless networks. This chapter elaborates the flaws in Wireless networks, and also confers about the tools, which can be used to find out whether the current deployment of wireless network is vulnerable for an attack. Due to the complexity of preventive measures, the TKIP and AES- CCMP are discussed in-depth.

In Chapter 2, the Mail Protocol and the vulnerabilities associated with the POP, IMAP and SMTP are explained. Format string vulnerability and the buffer overflow attacks are discussed in detail in this chapter. Vulnerability analysis requires checking the arguments of commands for malicious patterns. In case of SMTP traffic, the signatures will be checking for the SMTP commands as well as the

data in it. If the signatures are active in the data part of SMTP traffic, then it will result in dropping of a valid email thereby, resulting in a false positive. A case study of false positive in SMTP and IMAP traffic along with the algorithm to prevent the false positive is elaborated.

In Chapter 3, the FTP and TFTP protocol are explained. FTP protocol is prone to direct traversal attacks and buffer overflow attacks. The methods, which can be used to prevent these attacks, are also discussed. Structure of TFTP protocol with the opcodes and methods used to remove MS DOS device name attack, buffer overflow attack are also explained.

Chapter 4 deals with HTTP. Cross-site scripting attack, SQL injection attack and MS DOS Device name vulnerability are the most important attacks in HTTP. The intricacies of these attacks and the preventive measures of the attacks are discussed. Due to various encodings in HTTP, signatures are prone to evasion. As Oracle is the most commonly used database server, this chapter discusses the TNS protocol structure in detail. Methods to reduce false positive is represented with the help of flowchart and algorithm.

Chapter 5 deals with the structure of DNS /DHCP protocol and the algorithm. The algorithm ensures that the signatures (to prevent vulnerability in the protocol) are active only in the desired part of DNS/DHCP traffic. The algorithms aid in minimizing false positives. The chapter also details about the various attacks like DNS cache poisoning, DNS amplification attack and DNS hijacking attack.

Chapter 6 discusses the details of LDAP, SNMP and the ASN BER encoding. LDAP and SNMP protocol uses ASN, BER encoding. Understanding of ASN and BER syntax is required to identify the commands in LDAP and SNMP.

Chapter 7 focuses on the RPC protocol and the NDR encoding. The pseudo code of the algorithm, which ensures that the vulnerability specific rules are sanitized (only on specific parts of the RPC traffic) are discussed. The chapter discusses the Algorithm for both RPC over SMB and RPC over TCP. RPC traffic is prone to various evasions. The Port mapper in RPC is also elaborated.

Chapter 8 deals with malware. The chapter starts with the naming convention, which can be used for naming the malware. It then discusses about the confinement using hard virtual machines, soft virtual machines, jails, chroot, sensors and system call spoofing. The chapter then discusses about the rootkits, and preventive measures. The spyware and the preventive measures of Spyware are also discussed.

Chapter 9 focusses on reverse engineering. The chapter deals with linear sweep disassembler, recursive traversal disassembler and various evasion techniques, which can be used by disassembler. The detection of hardware break point, software break point and, detection of virtual machines are also presented. The chapter is concluded with the methods that are used to find the manual entry point of an executable and import table reconstruction.

The concepts that are discussed in this book is practical and will inculcate interest to the reader. To ensure a better understanding, the packet captures are taken from the real world exploits and the algorithms are presented in the form of flow charts. These algorithms can be converted into any language.

Although, the book has been designed for those who practice information security, the book can also be used for advance level network security courses. The instructors can feel free to contact.

Abhishek Singh

About Authors

Abhishek Singh

Abhishek is working as a Senior Software Engineer for SafeNet InfoTech Pvt. Ltd. In information security, his research interest is in IDS/IPS, firewall, cryptography, applied cryptography and VPN. Besides holding an invention disclosure in firewall, he holds one patent in two-factor authentication and another patent pending. He has authored chapters on VPN in Syngress title Firewall Policies and VPN Configurations (ISBN 1597490881). The book also appeared in 2008 Firewall Administrator's Professional CD (ISBN 1597492027).

Abhishek's research finding in the field of Compilers, Computer Networks, and Covert Channels has been published in primer conference and journals. He has also served in the review committee of ACSAC.

While pursuing his education he was employed with Symantec Corporation as a Senior Software Engineer, worked on a consulting project for Cypress Communication, which won third prize at 2004 turn around management competition. He has also held technical position with Third Brigade Security Center, research wing of Third Brigade.

He holds B.Tech in Electrical Engineering from IIT-BHU, Master of Science in Computer Science and Master of Science in Information Security from College of Computing Georgia Tech.

Baibhav Singh

Baibhav is currently working as a Software engineer for SafeNet. His area of expertise is in reverse engineering and in vulnerability assessment. He has provided expert consultancy to British Telecom and Tally Solutions for vulnerability assessment and in reverse engineering. He has also reported vulnerabilities to Microsoft and is one of the winners of Global Hacker 2007 Challenge competition.

Hirosh Joseph

Hirosh is currently working as a Security Researcher for Third Brigade, a Canada based information Security Company. He is one of the early members of Third Brigade Security Center and currently is one of the key member of the research team. He has more than five years of experience in Vulnerability research and is

passionate about reverse engineering, malware analysis and Spywares. He has also held security research position at Bluelane.