Security for Telecommunications Networks

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:

INSIDER ATTACK AND CYBER SECURITY: Beyond the Hacker edited by Salvatore Stolfo, Steven M. Bellovin, Angelos D. Keromytis, Sara Sinclaire, Sean W. Smith; ISBN: 978-0-387-77321-6

INTRUSION DETECTION SYSTEMS edited by Robert Di Pietro and Luigi V. Mancini; ISBN: 978-0-387-77265-3

VULNERABILITY ANALYSIS AND DEFENSE FOR THE INTERNET edited by Abhishek Singh; ISBN: 978-0-387-74389-9

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

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

Security for Telecommunications Networks

by

Patrick Traynor
Georgia Instutite of Technology, Atlanta, GA, USA

Patrick McDaniel
Thomas La Porta
Penn State University, University Park, PA, USA

Springer

Authors

Patrick Traynor
Georgia Institute of Technology
College of Computing
Mail code 0765
Atlanta, GA 30332-0765
traynor@cc.gatech.edu

Patrick McDaniel
Penn State University
Dept. Computer Science & Engineering
360A IST Bldg.
University Park PA 16802
mcdaniel@cse.psu.edu

Thomas La Porta
Penn State University
Dept. Computer Science & Engineering
360B IST Bldg.
University Park PA 16802
tlp@cse.psu.edu

Series Editor

Sushil Jajodia
George Mason University
Center for Secure Information Systems
4400 University Drive
Fairfax VA 22030-4444, USA
jajodia@gmu.edu

ISBN: 978-0-387-72441-6 e-ISBN: 978-0-387-72442-3

Library of Congress Control Number: 2008930147

Printed on acid-free paper

springer.com

For Mom, Dad, Tara and Sheila
–P.T.

For Megan, Sinclair, and Emerson
–P.M.

For Lisa, Abigail and Sophia
–T.L.

Contents

1 Introduction 1
1.1 Telecommunications Networks 2
1.2 Network Convergence and Security 3
1.3 Outline of this Book 4
1.4 Audience 5
1.5 Other Sources of Information 6

Part I Network Architecture

2 Security 9
2.1 Overview 9
2.1.1 What is security? 9
2.1.2 Basic Terminology 10
2.1.3 Attacks 11
2.1.4 Trust 11
2.2 Services and Tools 12
2.2.1 Cryptography 12
2.2.2 Authentication and Authorization 15
2.2.3 Certificates and PKI 16
2.3 Network Security 16
2.3.1 IPsec 16
2.3.2 SSL/TLS 18
2.3.3 Firewalls 19
2.3.4 Intrusion and Anomaly Detection 20
2.4 Summary 22

3 Cellular Architecture 23
3.1 History of Cellular Telephony 24
3.2 Cellular Voice Networks 26
3.2.1 Voice Network Elements 26

3.2.2 Home Location Register . . . 27
3.2.3 Mobile Switching Center/Visiting Location Register . . . 29
3.2.4 Base Station Subsystem . . . 29
3.3 Cellular Data Networks . . . 30
3.3.1 Data Network Elements . . . 30
3.3.2 Gateway GPRS Support Node . . . 31
3.3.3 Serving GPRS Support Node . . . 32
3.4 Signaling Network and Protocols . . . 33
3.4.1 Common Channel Signaling Network . . . 34
3.4.2 Message Transfer Part . . . 34
3.4.3 Signaling Connection Control Part . . . 35
3.4.4 Transaction Capabilities Application Part . . . 36
3.4.5 Mobile Application Part . . . 36
3.4.6 ISDN User Part . . . 36
3.5 Wireless Network . . . 36
3.5.1 Wireless Access Techniques . . . 37
3.5.2 Frequency Issues . . . 39
3.5.3 Voice Encoding . . . 43
3.5.4 Summary of Procedures . . . 45
3.6 Registration and Call Setup Procedures . . . 46
3.7 Core Network Security . . . 48
3.8 Air Interface Security . . . 49
3.9 Summary . . . 51

Part II Vulnerability Analysis

4 Vulnerabilities in the Telephony . . . 55
4.1 Weak Cryptographic Algorithms . . . 55
4.2 Vulnerabilities in the Network Core . . . 58
4.3 Wireless Eavesdropping . . . 60
4.4 Jamming . . . 61
4.5 User Tracking and Privacy . . . 62
4.6 Overload . . . 62
4.7 Malware . . . 63

5 Vulnerabilities in the Short Messaging Service (SMS) . . . 65
5.1 History and Description . . . 66
5.2 Delivering Messages . . . 66
5.2.1 Submitting a Message . . . 66
5.2.2 Routing a Message . . . 67
5.2.3 Wireless Delivery . . . 68
5.3 Identifying System Bottlenecks . . . 69
5.3.1 Queue Management . . . 70
5.3.2 Message Injection . . . 71

5.4 Efficient Device Targeting 72
5.4.1 NPA/NXX 73
5.4.2 Web Scraping 73
5.4.3 Testing Phone “Liveness” 74
5.4.4 Additional Collection Methods 75
5.5 Modeling Denial of Service 76
5.5.1 Attacking Individuals 76
5.5.2 Metropolitan Area Service 77
5.5.3 Regional Service 81
5.6 Network Characterization 82
5.7 Attack Characterization 85
5.8 Current Solutions 87
5.9 Queue Management 89
5.9.1 Weighted Fair Queuing 89
5.9.2 Weighted Random Early Detection 92
5.9.3 Summary 96
5.10 Resource Provisioning 96
5.10.1 Strict Resource Provisioning 97
5.10.2 Dynamic Resource Provisioning 100
5.10.3 Direct Channel Allocation 102
5.10.4 Summary 105
5.11 Combining Mechanisms 105
5.12 Summary 107

6 Vulnerabilities in Cellular Data Networks 109
6.1 History and Description 110
6.2 Delivering Packets from the Internet 111
6.2.1 Device Registration 111
6.2.2 Submitting Packets 112
6.2.3 Routing Packets 112
6.2.4 Wireless Delivery 113
6.3 Packet Multiplexing 115
6.4 Exploiting Cellular Data Services 116
6.4.1 Determining Network Settings 116
6.4.2 Exploiting Teardown Mechanisms 117
6.4.3 Exploiting Setup Mechanisms 121
6.5 Conflicts in Network Design 124
6.6 Efficient Mitigation of Data Network Vulnerabilities 129
6.7 Summary 130

7 Vulnerabilities in Voice over IP 133
7.1 History and Description 134
7.2 Session Initiation Protocol 135
7.2.1 Architecture 135
7.2.2 SIP Messages 136

7.2.3 Making Phone Calls 139
7.3 IP-Multimedia Subsystem Network 140
7.3.1 IMS Architecture 140
7.3.2 Making Phone Calls 141
7.4 IMS Versus Pure Internet Telephony 141
7.5 Wireless Issues 142
7.6 Security Issues 144
7.6.1 Current Solutions 145
7.6.2 Analysis of Emerging Vulnerabilities 148
7.7 Building Secure IP Telephony Networks 152
7.8 Summary 153

Part III Future Analyses

8 Future Directions and Challenges 157
8.1 Denial of Service Attacks 157
8.1.1 Logical vs Flooding Attacks 157
8.1.2 Problems in “Controlled” Networks 158
8.2 End-To-End Arguments and Security 159
8.3 The Future of Rigid Systems 160
8.4 Moving Forward 161

Glossary 163

References 167

Index 179