Praise for *Securing VoIP Networks*

"VoIP is part of the critical infrastructure. This excellent book highlights risks and describes mitigations. It could not have come more timely."

—Christian Wieser, OUSPG

"At a time when organizations are increasingly embracing VoIP as a major part of their communications infrastructure, the threat landscape is looking increasingly bleak. This book will enable its reader to look objectively at the real considerations surrounding securely deploying VoIP today. The authors are recognized experts in this field yet wear their learning lightly. The book is both authoritative yet easy to read. No mean feat!"

—Robert Temple, Chief Security Architect, BT Group

"The book provides a wealth of information on VoIP components and specific threats and vulnerabilities. Instead of a generic discussion, it presents a comprehensive set of security techniques and architectures to address VoIP risks."

—John Kimmins, Telcordia Fellow

"Recent massive Denial of Service attacks against Estonia (starting April 27, 2007) and YLE, Finland's national public service broadcasting company, (starting May 15, 2007) have made it clear it is better to act proactively. Read this book and prepare before it is too late."

—Prof. Juha Röning , University of Oulu
Principal Investigator of Oulu University Secure Programming Group (OUSPG) Head of Department of Electrical Engineering

SECURING VoIP NETWORKS

SECURING VoIP NETWORKS

THREATS, VULNERABILITIES, AND COUNTERMEASURES

Peter Thermos and Ari Takanen

Addison-Wesley

Upper Saddle River, NJ • Boston • Indianapolis • San Francisco
New York • Toronto • Montreal • London • Munich • Paris • Madrid
Cape Town • Sydney • Tokyo • Singapore • Mexico City

Library of Congress Cataloging-in-Publication Data:

Thermos, Peter.

Securing VoIP networks : threats, vulnerabilities, countermeasures / Peter Thermos and Ari Takanen.

p. cm.

ISBN 0-321-43734-9 (pbk. : alk. paper) 1. Internet telephony—Security measures. I. Takanen, Ari. II. Title.

TK5105.8865.H54 2007

004.695—dc22

2007017689

ISBN-13: 978- 0-321-43734-1
ISBN-10: 0-321-43734-9
Text printed in the United States on recycled paper at Courier in Stoughton, Massachusetts

First printing August, 2007

Editor-in-Chief: Karen Gettman
Acquisitions Editor: Chuck Toporek
Development Editor: Songlin Qiu
Managing Editor: Gina Kanouse
Project Editor: George E. Nedeff
Copy Editor: Keith Cline
Indexer: Lisa Stumpf
Proofreader: Megan Wade
Publishing Coordinator: Jamie Adams
Cover Designer: Chuti Prasertsith
Composition: Bronkella Publishing

To our families: Peter dedicates this book to Elaine, Anastasios, and Dionysia, and Ari wants to dedicate this book especially to Anu and our newborn girl.

Also we both would like to dedicate this book to all the experts and specialists who remain anonymous but are willing to share their knowledge and wisdom and enable the rest of us to learn and improve.

CONTENTS

Chapter 1: Introduction 1
Chapter 2: VoIP Architectures and Protocols 29
Chapter 3: Threats and Attacks 53
Chapter 4: VoIP Vulnerabilities 127
Chapter 5: Signaling Protection Mechanisms 165
Chapter 6: Media Protection Mechanisms 217
Chapter 7: Key Management Mechanisms 231
Chapter 8: VoIP and Network Security Controls 263
Chapter 9: A Security Framework for Enterprise VoIP Networks . .297
Chapter 10: Provider Architectures and Security 315
Chapter 11: Enterprise Architectures and Security 334
Index 345

CONTENTS

Foreword xiv
Preface xvii
Acknowledgments xx
About the Authors xxiii

Chapter 1: Introduction 1

VoIP and Telecommunications 4
VoIP and IP Communications 9
VoIP Deployments 12
Challenges in VoIP Security 15
Risk Analysis for VoIP 18
VoIP as Part of IT and the Security Organization 21
Security Certifications 23
Summary 25

Chapter 2: VoIP Architectures and Protocols 29

Architectures 32
VoIP Network Components 41
Signaling Protocols 44
Media Transport Protocols 49
Other IP Protocols Used in VoIP 50
Summary 51

Chapter 3: Threats and Attacks 53

Definitions of Threats and Attacks 53
Threats in VoIP 56
Service Disruption 59
Attacks Related to Telephony Services 61
Denial of Service 64

Annoyance (That Is, SPIT) 75
Unauthorized Access 76
Eavesdropping 84
Masquerading 101
Fraud 113
Summary 125

Chapter 4: VoIP Vulnerabilities 127

Categories of Vulnerabilities 127
Configuration Management Vulnerabilities in VoIP 159
Approaches to Vulnerability Analysis 160
Human Behavior Vulnerabilities 162
Summary 163

Chapter 5: Signaling Protection Mechanisms 165

SIP Protection Mechanisms 166
Transport Layer Security 176
Datagram Transport Layer Security 183
S/MIME 186
IPSec 190
H.323 Protection Mechanisms 193
MGCP Protection Mechanisms 214
Summary 216

Chapter 6: Media Protection Mechanisms 217

SRTP 218
SRTCP 227
Summary 229

Chapter 7: Key Management Mechanisms 231

MIKEY 234
SRTP Security Descriptions 247
ZRTP 251
Summary 261

Chapter 8: VoIP and Network Security Controls 263

Architectural Considerations 264
Authentication, Authorization, and Auditing: Diameter 270
User-Authorization-Request Command 278
VoIP Firewalls and NAT 280
Session Border Controllers 282
Intrusion Detection and VoIP 289
Summary 295

Chapter 9: A Security Framework for Enterprise VoIP Networks . .297

VoIP Security Policy 298
External Parties 299
Asset Management 301
Physical and Environmental Security 301
Equipment Security 302
Operations Management 304
Access Control 307
Information Systems Acquisition, Development, and Maintenance 311
Security Incident Management 312
Business Continuity Management 313
Compliance 313
Summary 314

Chapter 10: Provider Architectures and Security 315

Components 315
Network Topologies 319
Security in Provider Implementations 327
Summary 333

Chapter 11: Enterprise Architectures and Security 335

Components 335
Network Topologies 338
Security Considerations 343
Summary 344

Index 345

FOREWORD

I have been teaching computer engineering in courses like Software Engineering and Operating Systems for more than 20 years. In all my teaching I have stressed making students understand the principles of the focal area of a course and not just having them memorize one technique or another. The increasing complexity of networks and our whole information society challenges this understanding even more. Different parts of the information structure can communicate with each other and understand each other via communication protocols. This opens up new threats in communication networks. Vulnerability in any of the communication protocols may make the whole system weak. It is of utmost importance that our developers and experts today and tomorrow have a good understanding of security aspects and can apply them.

Tomorrow, all communications will happen over IP. In the past, telecom operators handled most communications, and the main business for them was voice communication. In reality, almost all last-mile communications today still happen over the conventional telecom infrastructure. The backbone of the Internet has been going through a fast transition to faster and faster fiber optics and digital data transfer. The era of analog communications has been over for some time already. But, there are other changes in the communications landscape. I will describe some of them based on experiences we have had as one of the most advanced high-tech countries. This is so because here in Oulu, Finland, we have been surrounded by high-tech inventions, and several enterprises use the city as a test bed for their inventions and their business models.

In the past, the first GSM network was launched in Oulu. GSM technology took over the communications landscape quickly, and today in Finland we have people in their thirties who have never in their life owned a fixed-line telephone. Today there are more cellular phones in Finland than there are people. Less than 50% of households have a fixed-line phone, and the number of fixed-line connections is still dropping faster every year.

At the same time, the transition from fixed-line voice communications to fixed-line data communications has happened very rapidly globally. Most households now subscribe to broadband service, and they use services such as e-mail and the web in their everyday life. Necessary cabling to the households existed due to the transition from fixed-line to mobile, and the cabling was reused by the broadband providers.

Today the transition is from providing services to providing bandwidth. Recently, the next step in breaking traditional business models was taken in Oulu. One of the first free WiFi networks was also launched here. With the introduction of WiFi-enabled cellular phones, consumers in Finland are testing various free VoIP services, and that might be the end of all voice-based business models. The transition from voice to data, and from fixed to mobile, results in personal, always connected wireless communication devices.

Today, people speak of Voice over IP, but a better name for the Next Generation Networks is Everything over IP (EoIP). And all of that communication will be wireless. But what does that have to do with the topic of this book? It means the world has to finally wake up to the security of the communications networks.

To build security, you have to understand the application you use. For many, Internet security equals web security. This false impression is created by security companies, the media, and the software industry. For many, an application is the same thing as a web application. Application security equals web application security. But today, the web is not the biggest threat to your business. True, some businesses are built on web services, but other applications such as e-mail and voice can be much more critical for enterprises and for consumers. Web security can have a high profile, as a compromised server is seen by hundreds of thousands of people. A compromised voice connection or e-mail client might escape public attention but could result in the loss of the most critical assets of a company, or cause irreversible damage to an individual.

To be secure, you have to understand that wireless networks are always open. While in traditional telephone networks all the switches were kept behind locked doors and all the cabling was protected, in wireless technology there are no cables and everyone has access to wireless access points. One compromised infrastructure component, and the entire network is compromised. One virus-contaminated access device, and everyone in the network will be contaminated.

To be secure, you have to understand that client security is as important as, or even more important, than server security. Servers can be protected, upgraded, and updated and potential damages can be restored. These are standard processes for all IT administrators. Now, take laptops as an example of a mobile device of the future. Most, if not all, critical data is stored on the laptop. All the keys and passwords are there. Communication behavior is stored there. The laptop also can eavesdrop on all behavior, including listening to the surroundings of the user of the laptop. A mobile device of the future is all that and more.

This book by Peter and Ari is built around voice as the application to be secured, but the principles apply to any communications. Studying this book should be obligatory to all students in computer engineering and computer science, not only due to its content and deep understanding of VoIP security, but also to allow them to learn how to apply the best practices in other fields, no matter what their future field of study will be. The key to learning is not only studying things and memorizing the various topics, but learning how to apply the best practices of other fields in your own. Combining the best practices of traditional telecommunications, e-mail, and the web into new next-generation technologies is essential to be able to build reliable and usable communication technologies. Voice over IP is potentially the killer application, destroying conventional communication networks and creating a new IP-based communication infrastructure. I truly hope it will not be built by business people only, but also by people who understand the security aspects of the new technologies.

Prof. Juha Röning
Principal Investigator of Oulu University Secure Programming Group (OUSPG)
Head of Department of Electrical Engineering
University of Oulu

May 30, 2007

PREFACE

Communication between people has changed with the invention of the telephone. The ability to communicate across continents in real-time has also helped our society in several dimensions including entertainment, trade, finance, and defense. But this new capability did not come without an investment. Building an international telephony infrastructure has required the cooperation of both commercial and government organizations to evolve into what it is today. It has also led to the formation of international standard bodies that both direct and support the industry towards an interoperable communication networks.

IP networks are the next step from the traditional telecommunications. For a while, IP family of protocols was only used in the Internet, and the main applications were file transfers and e-mail. With the World Wide Web, the Internet changed into a global and always open information distribution channel. And finally with the advent of VoIP, the Internet is becoming a real-time communication media that integrates with all the earlier multimedia capabilities.

Traditional telecommunication networks are critical to the survival of our society. The PSTN is a closed network and its operational intricacies are known to a few select individuals who have devoted much of their lives to building it. Although operations in PSTN are not entirely a secret, they were and still remain proprietary for several reasons such as competitive advantage and national defense. The PSTN was and remains a closed infrastructure that concentrated its intelligence in its core network elements and left the edge devices very simplistic. The equipment and resources to operate a TDM network require a substantial financial investment. This lack of direct access to core network elements from subscribers and the high price of connectivity alleviated the risk for attacks. Ergo, subscribers demonstrate greater trust for communications through the PSTN compared to the Internet. This is a misconceived trust once you start analyzing the PSTN components and protocols and realize the lack of protection mechanisms.

In the earlier days of the Internet, security was appalling. The Internet was an open network where anyone could attack anyone anonymously and many of the attack tools were, and still are, available. As such, security research became a standard practice in government, commercial, and academic worlds with globally known research groups in organizations such as DARPA, DISA, CERIAS, MIT CIS, Bellcore, Bell Labs, and many others. Things became a bit more complicated with the transition of critical services such as telephony on the Internet along with other multimedia applications such as video and gaming. And due to the performance, availability, and privacy requirements of these applications, their security requires new approaches and methods compared to traditional IP security. Nevertheless the traditional security objectives apply such as confidentiality, integrity, and availability of services.

Before gaining the interest of the academia, the topic of Internet security has been a secret science, or not even a science. The security field was a competition between hackers and system administrators, in a constant race of "patch and penetrate." Very few people knew what they actually were fixing in the systems when they applied new security updates or patches. And very few hackers understood what the attack tools actually did when they penetrated the services they wanted access to. People spoke of threats, attacks, and security measures that needed to be applied to protect from these attacks. The actual core reasons that enabled the existence of the attacks were not understood. For most of the users of communication systems, these weaknesses were hidden in complex, hard-to-understand protocols and components used in the implementations.

VoIP has been discussed at length in many textbooks and thus we avoid long discussions of its origins and details on introductory concepts. Instead the book focuses on the details associated with the security of multimedia communications including VoIP. Our purpose is to extend your knowledge of vulnerabilities, attacks, and protection mechanisms of VoIP and generally Internet multimedia applications. We deviate from listing a series of security tools and products and instead provide detailed discussions on actual attacks and vulnerabilities in the network design, implementation, and configuration and protection mechanisms for signaling and media streams, architectural recommendations, and organizational strategy—thus enabling you to understand and implement the best countermeasures that are applicable to your environment.

The book is structured so that we start by briefly explaining VoIP networks, and then go through the threats, attacks, and vulnerabilities to

enable you to understand how VoIP attacks are made possible and their impact. The book discusses in great detail various attacks (published and unpublished) for eavesdropping, unauthorized access, impersonation, and service disruption. These attacks are used as proof of concept, but at the same time they also expose the reader to real-life weaknesses and serve as a mechanism to promote comprehension. In addition, this book discusses VoIP vulnerabilities, their structure, and their categorization as they have been investigated in enterprise and carrier environments.

Following VoIP vulnerabilities and attacks, the book discusses in great detail a number of protection mechanisms. In order to protect against current and emerging threats, there a number of areas that need to be considered when deploying VoIP. The book provides extensive coverage on the intricacies, strengths, and limitations of the protection mechanisms including SIPS, H.235, SRTP, MIKEY, ZTP, and others. Furthermore, the book focuses on identifying a VoIP security framework as a starting point for enterprise networks and provides several recommendations. Security architectures in enterprise and carrier environments are also discussed.

This first edition of the book aims in establishing the landscape of the current state of VoIP security and provides an insight to administrators, architects, security professionals, management personnel, and students who are interested in understanding VoIP security in detail.

ACKNOWLEDGMENTS

First, we both would like to acknowledge IETF and everyone participating in the work of IETF for their great work for VoIP and all communication standards. A portion of the proceeds is donated to IETF to support their efforts in standardizing the Internet. Keep up the good work!

Additional Acknowledgments from Peter Thermos

I have been fortunate to be acquainted with many people in the professional and academic community who generously shared their knowledge and experience throughout my career. These people have inspired me to research new topics and in turn share some of my experience and knowledge in the area of VoIP security with this book. I would like to thank them and I hope that I can inspire others including students and professionals to explore this field.

I would like to thank Henning Schulzrinne for his continuous support and academic guidance, John Kimmins for his professional wisdom and advisement, and Emmanuel Lazidis for the numerous and prolific discussions on information security. Also I would like to thank several people in two U.S. agencies that supported early research in the area of next-generation networks and security including Bill Semancik, Linda Shields, Gary Hayward, Tom Chapuran (Telcordia), David Gorman at LTS (Laboratory for Telecommunications Sciences), and Tim Grance and Richard Kuhn at NIST along with Dave Waring, Tom Bowen, Steve Ungar and John Lutin at Telcordia.

In addition, I would like to thank our reviewers John Haluska, Paul Rohmeyer, and Christian Wieser for their valuable comments and feedback. Also I would like to thank the many supporters of the VoPSecurity.org Forum and Dan York and Jonathan Zar for their community contribution of the BlueBox, The VoIP Security podcast. Furthermore, I would like to thank you, our reader, for your generosity and support. We welcome your comments and feedback!

Lastly but most importantly I would like to thank my beautiful wife Elaine and children Anastasios and Dionysia for their understanding and support during the writing of this book. The reader will appreciate the fact that the manuscript reads mostly in English and not Greek, which is largely due to the continuous support of my wife's instruction (an English teacher) in writing proper English!

Additional Acknowledgments from Ari Takanen:

There have been several people that have paved the way towards the writing of this book. Great thanks to Marko Laakso and Prof. Juha Röning from University of Oulu for showing me how everything is broken in communication technologies. Everything. And showing that there is no silver bullet to fix that. My years as a researcher in the PROTOS project in the OUSPG enabled me to learn everything there was to learn about communications security. Out of all those communication technologies we were studying, one family of protocols stood out like a shining supernova: VoIP. Thank you to all Oulu University Secure Programming Group members for all the bits and pieces around VoIP security. I know we did not cover all of them in the book, but let's leave something for the future researchers also! And a special thanks to Christian Wieser who did not get bored of VoIP after learning it, like many others did, but kept on focusing on VoIP security among all those hundreds of other interesting communication technologies being studied in the research team. Thank you Christian for all the help in putting this book together!

Enormous thanks to all my colleagues at Codenomicon, for taking the OUSPG work even further through commercializing the research results, and for making it possible for me to write this book although it took time from my CTO tasks. Thank you to everyone who has used either the Codenomicon robustness testing tools or the PROTOS test-suites, and especially to everyone who came back to us and told us of their experiences with our tools and performing VoIP security testing with them. Although you might not want to say it out loud, you certainly know how broken everything is.

Special thanks to Jeff Pulver and Carl Ford out of Pulver.com for your significant work in making VoIP what it is today, and for inviting me to speak in more than ten different conferences that you have arranged.

Through meetings with all key people in VoIP (a list too long to fit on one page), these conferences were probably the best learning experience for me in the VoIP area. I am terribly sorry for the time it took for me to understand that pointing out the problems was not the correct way of preaching but rather pointing out the solutions. I hope we contributed to the latter in this book!

I would like to thank everyone involved at Addison-Wesley and Pearson Education, and all the other people who patiently helped with all the editing and reviewing, and impatiently reminded me about all the missed deadlines during the process.

Finally, thanks Peter for inviting me into this project, although it was slow and painful at times, it certainly was more fun than anything else, and I will definitely do it again!

About the Authors

Peter Thermos is CTO at Palindrome Technologies, which acts as a trusted advisor for commercial and government organizations and provides consultation in security policy, architecture, and risk management. Previously Peter acted as Telcordia's lead technical expert on key information security and assurance tasks, including risk assessments, standards and requirements development, network security architecture, and organizational security strategy. He speaks frequently at events and forums including the IEEE, MIS, Internet Security Conference, SANS, ISSWorld, IEC, the 21st Century Communications World Forum, VON, and others. Peter is also known for his contributions to the security community through discovery of product vulnerabilities, the release of SiVuS (The First VoIP Vulnerability Scanner), and the vopsecurity.org forum. Peter holds a masters' degree in computer science from Columbia University where he is currently furthering his graduate studies.

Ari Takanen is founder and CTO of Codenomicon. Since 1998, Ari has focused on information security issues in next-generation networks and security critical environments. He began at Oulu University Secure Programming Group (OUSPG) as a contributing member to PROTOS research that studied information security and reliability errors in WAP, SNMP, LDAP, and VoIP implementations. Ari and his company, Codenomicon Ltd., provide and commercialize automated tools using a systematic approach to test a multitude of interfaces on mission-critical software, VoIP platforms, Internet-routing infrastructure, and 3G devices. Codenomicon and the University of Oulu aim to ensure new technologies are accepted by the general public by providing means of measuring and ensuring quality in networked software. Ari has been speaking at numerous security and testing conferences on four continents and has been invited to speak at leading universities and international corporations.