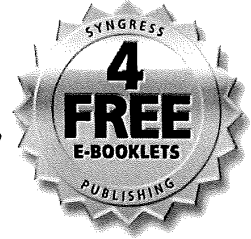


SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP



HOW TO CHEAT AT VoIP Security

The Perfect Reference for the Multitasked SysAdmin

- Discover Why “Measure Twice, Cut Once” Applies to Securing a VoIP Infrastructure
- Learn How to Secure an Entire VoIP Infrastructure and Defend Against Denial-of-Service and Hijacking Attacks
- The Perfect Guide if VoIP Engineering is NOT Your Specialty

Thomas Porter
Michael Gough

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Syngress Publishing, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

| KEY | SERIAL NUMBER |
|-----|---------------|
| 001 | HJIRTCV764 |
| 002 | PO9873D5FG |
| 003 | 829KM8NJH2 |
| 004 | VTY45Q9PLA |
| 005 | CVPLQ6WQ23 |
| 006 | VBP965T5T5 |
| 007 | HJJJ863WD3E |
| 008 | 2987GVTWMK |
| 009 | 629MP5SDJT |
| 010 | IMWQ295T6T |

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

How to Cheat at VoIP Security

Copyright © 2007 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0

ISBN 10: 1-59749-169-1
ISBN 13: 978-1-59749-169-3

Publisher: Amorette Pedersen
Acquisitions Editor: Gary Byrne
Technical Editor: Thomas Porter
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien
Copy Editors: Adrienne Rebello, Mike
McGee
Indexer: Nara Wood

Distributed by O'Reilly Media, Inc. in the United States and Canada.
For information on rights, translations, and bulk sales, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.

Contents

| | |
|--|-----------|
| Chapter 1 Introduction to VoIP Security | 1 |
| Introduction | .2 |
| The Switch Leaves the Basement | .4 |
| What Is VoIP? | .6 |
| VoIP Benefits | .6 |
| VoIP Protocols | .8 |
| VoIP Isn't Just Another Data Protocol | .9 |
| Security Issues in Converged Networks | .11 |
| VoIP Threats | .14 |
| A New Security Model | .15 |
| Summary | .16 |
| Chapter 2 The Hardware Infrastructure | 19 |
| Introduction | .20 |
| Traditional PBX Systems | .21 |
| PBX Lines | .22 |
| PBX Trunks | .24 |
| PBX Features | .25 |
| PBX Adjunct Servers | .28 |
| Voice Messaging | .28 |
| Interactive Voice Response Servers | .29 |
| Wireless PBX Solutions | .30 |
| Other PBX Solutions | .30 |
| PBX Alternatives | .30 |
| VoIP Telephony and Infrastructure | .31 |
| Media Servers | .31 |
| Interactive Media Service: Media Servers | .32 |
| Call or Resource Control: Media Servers | .32 |
| Media Gateways | .33 |
| Firewalls and Application-Layer Gateways | .34 |
| Application Proxies | .34 |
| Endpoints (User Agents) | .35 |
| IP Switches and Routers | .38 |
| Wireless Infrastructure | .38 |
| Wireless Encryption: WEP | .38 |

| | |
|--|------------|
| Wireless Encryption: WPA2 | .39 |
| Authentication: 802.1x | .40 |
| Power-Supply Infrastructure | .41 |
| Power-over-Ethernet (IEEE 802.3af) | .41 |
| UPS | .42 |
| Energy and Heat Budget Considerations | .43 |
| Summary | .44 |
| Chapter 3 Architectures | .45 |
| Introduction | .46 |
| PSTN: What Is It, and How Does It Work? | .46 |
| PSTN: Outside Plant | .46 |
| PSTN: Signal Transmission | .49 |
| T1 Transmission: Digital Time Division Multiplexing | 49 |
| PSTN: Switching and Signaling | .55 |
| The Intelligent Network (IN), Private Integrated Services, ISDN, and QSIG | .56 |
| ITU-T Signaling System Number 7 (SS7) | .57 |
| PSTN: Operational and Regulatory Issues | .61 |
| PSTN Call Flow | .61 |
| PSTN Protocol Security | .64 |
| SS7 and Other ITU-T Signaling Security | .64 |
| ISUP and QSIG Security | .66 |
| The H.323 Protocol Specification | .67 |
| The Primary H.323 VoIP-Related Protocols | .68 |
| H.225/Q.931 Call Signaling | .71 |
| H.245 Call Control Messages | .75 |
| Real-Time Transport Protocol | .77 |
| H.235 Security Mechanisms | .78 |
| Understanding SIP | .82 |
| Overview of SIP | .83 |
| RFC 2543 / RFC 3261 | .84 |
| SIP and Mbone | .85 |
| OSI | .85 |
| SIP Functions and Features | .87 |
| User Location | .88 |
| User Availability | .88 |
| User Capabilities | .88 |
| Session Setup | .89 |

Session Management 89
 SIP URIs 89
 SIP Architecture 90
 SIP Components 90
 User Agents 90
 SIP Server 91
 Stateful versus Stateless 92
 Location Service 92
 Client/Server versus Peer-to-Peer Architecture 93
 Client/Server 93
 Peer to Peer 94
 SIP Requests and Responses 94
 Protocols Used with SIP 97
 UDP 97
 Transport Layer Security 98
 Other Protocols Used by SIP 99
 Understanding SIP's Architecture 102
 SIP Registration 102
 Requests through Proxy Servers 103
 Requests through Redirect Servers 103
 Peer to Peer 104
 Instant Messaging and SIMPLE 105
 Instant Messaging 106
 SIMPLE 107
 Summary 109
Chapter 4 Support Protocols 111
 Introduction 112
 DNS 112
 DNS Architecture 113
 Fully Qualified Domain Name 114
 DNS Client Operation 115
 DNS Server Operation 116
 Security Implications for DNS 117
 TFTP 118
 TFTP Security Concerns 118
 TFTP File Transfer Operation 119
 Security Implications for TFTP 119
 HTTP 120
 HTTP Protocol 121

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.