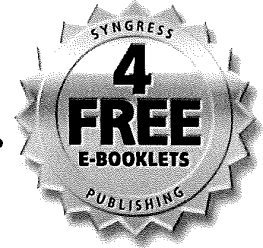


SYNGRESS®

**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](mailto:matt@syngress.com) or fax to 781-681-3585.

# Contents

<b>Chapter 1 Introduction to VoIP Security</b>	<b>1</b>
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
<b>Chapter 2 The Hardware Infrastructure</b>	<b>19</b>
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
<b>Chapter 3 Architectures .....</b>	<b>45</b>
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
<b>Chapter 4 Support Protocols .....</b>	<b>111</b>
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

HTTP Client Request .....	121
HTTP Server Response .....	122
Security Implications for HTTP .....	122
SNMP .....	123
SNMP Architecture .....	124
SNMP Operation .....	124
SNMP Architecture .....	125
DHCP .....	126
DHCP Protocol .....	126
DHCP Operation .....	127
Security Implications for DHCP .....	128
RSVP .....	129
RSVP Protocol .....	130
RSVP Operation .....	130
Security Implications for RSVP .....	131
SDP .....	132
SDP Specifications .....	132
SDP Operation .....	133
Security Implications for SDP .....	134
Skinny .....	135
Skinny Specifications .....	135
Skinny Operation .....	135
Security Implications for Skinny .....	136
Summary .....	138
<b>Chapter 5 Threats to VoIP Communications Systems . .</b>	<b>141</b>
Introduction .....	142
Denial-of-Service or VoIP Service Disruption .....	142
Call Hijacking and Interception .....	148
ARP Spoofing .....	151
H.323-Specific Attacks .....	155
SIP-Specific Attacks .....	156
Summary .....	157
<b>Chapter 6 Confirm User Identity .....</b>	<b>159</b>
Introduction .....	160
802.1x and 802.11i (WPA2) .....	163
802.1x/EAP Authentication .....	164
Supplicant (Peer) .....	164
Authenticator .....	164

Authentication Server .....	164
EAP Authentication Types .....	167
EAP-TLS .....	169
EAP-PEAP .....	171
EAP-TTLS .....	171
PEAPv1/EAP-GTC .....	171
EAP-FAST .....	171
LEAP .....	172
EAP-MD-5 .....	172
Inner Authentication Types .....	173
Public Key Infrastructure .....	175
Public Key Cryptography Concepts .....	176
Architectural Model and PKI Entities .....	178
Basic Certificate Fields .....	180
Certificate Revocation List .....	181
Certification Path .....	181
Minor Authentication Methods .....	182
MAC Tools .....	182
MAC Authentication .....	183
ARP Spoofing .....	183
Port Security .....	183
Summary .....	183
<b>Chapter 7 Active Security Monitoring .....</b>	<b>185</b>
Introduction .....	186
Network Intrusion Detection Systems .....	187
NIDS Defined .....	187
Components .....	188
Types .....	189
Placement .....	191
Important NIDS Features .....	194
Maintenance .....	194
Alerting .....	194
Logging .....	194
Extensibility .....	194
Response .....	194
Limitations .....	195
Honeypots and Honeynets .....	195
Host-Based Intrusion Detection Systems .....	196

Logging .....	197
Syslog .....	197
SNMP .....	199
What Is a Penetration/Vulnerability Test? .....	200
Methodology .....	201
Discovery .....	201
Scanning .....	202
Vulnerability Assessment .....	203
Exploitation .....	203
Reporting .....	203
Summary .....	205
<b>Chapter 8 Logically Segregate Network Traffic .....</b>	<b>207</b>
Introduction .....	208
VLANs .....	209
VLAN Security .....	212
VLANs and Softphones .....	212
QoS and Traffic Shaping .....	214
NAT and IP Addressing .....	215
How Does NAT Work? .....	216
NAT Has Three Common Modes of Operation .....	218
NAT and Encryption .....	221
NAT as a Topology Shield .....	225
Firewalls .....	225
A Bit of Firewall History .....	226
Shallow Packet Inspection .....	226
Stateful Inspection .....	227
Medium-Depth Packet Inspection .....	227
Deep Packet Inspection .....	228
VoIP-Aware Firewalls .....	229
H.323 Firewall Issues .....	230
SIP Firewall Issues .....	231
Bypassing Firewalls and NAT .....	232
Access Control Lists .....	235
Summary .....	237
<b>Chapter 9 IETF Encryption Solutions for VoIP .....</b>	<b>239</b>
Introduction .....	240
Suites from the IETF .....	240
S/MIME: Message Authentication .....	241



S/MIME Messages .....	244
Sender Agent .....	244
Receiver Agent .....	244
E-mail Address .....	244
TLS: Key Exchange and Signaling Packet Security .....	244
Certificate and Key Exchange .....	245
SRTP: Voice/Video Packet Security .....	247
Multimedia Internet Keying .....	248
Session Description Protocol Security Descriptions ...	248
Providing Confidentiality .....	248
Message Authentications .....	249
Replay Protection .....	250
Summary .....	251
<b>Chapter 10 Skype Security .....</b>	<b>253</b>
Security .....	254
Blocking Skype .....	257
Firewalls .....	257
Downloads .....	257
Software Inventory and Administration .....	258
Firewalls .....	258
Proxy Servers .....	260
Embedded Skype .....	260
A Word about Security .....	260
<b>Chapter 11 Skype Firewall and Network Setup .....</b>	<b>263</b>
A Word about Network Address Translation and Firewalls ..	264
Home Users .....	266
Small to Medium-Sized Businesses .....	266
Large Corporations .....	267
What You Need to Know	
About Configuring Your Network Devices .....	269
Home Users or Businesses	
Using a DSL/Cable Router and No Firewall .....	269
Small to Large Company Firewall Users .....	269
TCP and UDP Primer .....	269
NAT vs. a Firewall .....	270
Ports Required for Skype .....	271
Home Users or Businesses	
Using a DSL/Cable Router and No Firewall .....	271

Small to Large Company Firewall Users .....	271
Skype's Shared.xml file .....	273
Microsoft Windows Active Directory .....	273
Using Proxy Servers and Skype .....	276
Wireless Communications .....	277
Display Technical Call Information .....	278
Small to Large Companies .....	282
How to Block Skype in the Enterprise .....	282
Endnote .....	283
<b>Appendix A Validate Existing Security Infrastructure</b>	<b>285</b>
Introduction .....	286
Security Policies and Processes .....	287
Physical Security .....	297
Perimeter Protection .....	300
Closed-Circuit Video Cameras .....	300
Token System .....	300
Wire Closets .....	301
Server Hardening .....	301
Eliminate Unnecessary Services .....	302
Logging .....	303
Permission Tightening .....	304
Additional Linux Security Tweaks .....	306
Activation of Internal Security Controls .....	308
Security Patching and Service Packs .....	312
Supporting Services .....	313
DNS and DHCP Servers .....	313
LDAP and RADIUS Servers .....	315
NTP .....	315
SNMP .....	316
SSH and Telnet .....	317
Unified Network Management .....	317
Sample VoIP Security Policy .....	318
Purpose .....	319
Policy .....	319
Physical Security .....	319
VLANs .....	319
Softphones .....	319

Encryption .....	319
Layer 2 Access Controls .....	320
Summary .....	321
<b>Appendix B The IP Multimedia Subsystem: True Converged Communications .....</b>	<b>323</b>
Introduction .....	324
IMS Security Architecture .....	325
IMS Security Issues .....	328
SIP Security Vulnerabilities .....	329
Registration Hijacking .....	329
IP Spoofing/Call Fraud .....	329
Weakness of Digest Authentication .....	329
INVITE Flooding .....	329
BYE Denial of Service .....	330
RTP Flooding .....	330
Spam over Internet Telephony (SPIT) .....	330
Early IMS Security Issues .....	330
Full IMS Security Issues .....	331
Summary .....	332
Related Resources .....	332
<b>Appendix C Regulatory Compliance .....</b>	<b>333</b>
Introduction .....	334
SOX: Sarbanes-Oxley Act .....	336
SOX Regulatory Basics .....	336
Direct from the Regulations .....	336
What a SOX Consultant Will Tell You .....	338
SOX Compliance and Enforcement .....	341
Certification .....	341
Enforcement Process and Penalties .....	342
GLBA: Gramm-Leach-Bliley Act .....	342
GLBA Regulatory Basics .....	343
Direct from the Regulations .....	343
What a Financial Regulator or GLBA Consultant Will Tell You .....	347
GLBA Compliance and Enforcement .....	349
No Certification .....	350
Enforcement Process and Penalties .....	350

HIPAA: Health Insurance	
Portability and Accountability Act .....	351
HIPAA Regulatory Basics .....	351
Direct from the Regulations .....	351
What a HIPAA Consultant Will Tell You .....	358
HIPAA Compliance and Enforcement .....	359
No Certification .....	359
Enforcement Process and Penalties .....	359
CALEA: Communications Assistance	
for Law Enforcement Act .....	360
CALEA Regulatory Basics .....	363
Direct from the Regulations .....	364
What a CALEA Consultant Will Tell You .....	375
CALEA Compliance and Enforcement .....	376
Certification .....	376
Enforcement Process and Penalties .....	377
E911: Enhanced 911 and Related Regulations .....	377
E911 Regulatory Basics .....	378
Direct from the Regulations .....	378
What an E911 Consultant Will Tell You .....	382
E911 Compliance and Enforcement .....	383
Self-Certification .....	383
Enforcement Process and Penalties .....	383
EU and EU Member States'	
eCommunications Regulations .....	384
EU Regulatory Basics .....	385
Direct from the Regulations .....	385
What an EU Data Privacy Consultant Will Tell You .....	389
EU Compliance and Enforcement .....	390
No Certification .....	390
Enforcement Process and Penalties .....	390
Summary .....	390

## Are You Owned?

### Consumer Softphone Gotchas

Many consumer-oriented softphones contain advertising software that “phones home” with private user information. Several popular softphones (such as X-Lite) store credentials unencrypted in the Window's registry even after uninstallation of the program. Softphones require that PC-based firewalls open a number of high UDP ports as part of the media stream transaction. Additionally, any special permissions that the VoIP application has within the host-based firewall rule set will apply to all applications on that desktop (e.g., peer-to-peer software may use SIP for bypassing security policy prohibitions).

Also consider that malware affecting any other application software on the PC can also interfere with voice communications. The flip-side is also true—malware that affects the VoIP software will affect all other applications on the PC and the data services available to that PC (a separate VoIP phone would not require access to file services, databases, etc.).

### IM Clients

Instant messaging is perhaps the dominant means of real-time communication on the Internet today. IM's roots can be traced back to the Internet Relay Chat (IRC) networks, which introduced the chat room concept but did not track online presence and never reached the popularity of IM. Just as IM is the next logical step from IRC, voice chat is the next leap from text-based chat. Most of today's most popular IM clients have included voice functionality, including AOL's Instant Messenger, Yahoo! Messenger, and MSN Messenger. Skype took the opposite approach and created a chat client that focuses on voice as the star and text chat as an afterthought. Even Google jumped aboard the IM bandwagon, releasing Google Talk. Let's take a look at these clients to see what makes them similar, and what makes them different.

AIM, AOL's IM service, surely wasn't the first on the scene, but it has the largest base of users. Initially AIM was limited to users of the AOL Internet service, but eventually it was opened up to the Internet as a whole. With the addition of a proprietary voice capability in late 1999, AOL was a VoIP pioneer of sorts. (although voice chat was first available through Mirablis's ICQ). Yahoo! Chat jumped aboard the voice bandwagon soon after, and Google's more recent client has included voice from the beginning. In 2005, Yahoo announced interoperability with Google and MSN (who also has a voice chat plug-in for messenger that is also used with its Live Communication Server product). In addition, Microsoft's popular

[www.syngress.com](http://www.syngress.com)

Outlook e-mail client (and entire Office suite in the case of LCS) can be linked to Microsoft Messenger. Also worth mentioning is the Lotus Domino IM client that competes with Microsoft LCS in the enterprise instant messaging (and presence) space, as well as Jabber, which can be used to tie together both public and private IM services using the XMPP protocol.

Google Talk is the newest comer to the IM game. Though Google Talk is still in its infancy, it stands to succeed due largely to a philosophical stand point, embracing open standards over proprietary voice chat. Google Talk aims to connect many different voice networks over a series of peering arrangements, allowing users to minimize their need to run several IM clients. Like Skype, Google seeks to bridge traditional phone calls with Internet telephony, promising to federate with SIP networks that provide access to an ordinary telephone dial tone. Google recently released a library called libjingle to programmers, allowing them to hack new functionality into Google Talk. It will be interesting to see where Google takes Google Talk in the future.

### *Video Clients*

Most of us can probably think back and recall seeing episodes of *The Jetsons* when we were younger. Or pictures of the AT&T PicturePhone from the 1964 World's Fair. Movies have all but promised these devices to be a staple of every day life in the future. And for decades, the video conference has been pushed by enterprises seeking to save money on travel (though investments in video conferencing equipment tend to sit around gathering dust). Live video on the Internet has its adherents, and today we see yet another wave of marketing aimed at the business use of video. So, will video finally take off around VoIP just like audio, or is there something different going on here?

The video phone has been tomorrow's next big technology for 50 years but the issue has been more sociological than technological. Certainly, popular instant messaging clients have included video chat capabilities for some time now, although each client typically supports only video between other users of the same client or messaging network. And although it always gives me a kick to see someone else announcing that they've solved the gap with technology, the point is well taken that video is here to stay in VoIP systems—even if it doesn't get as much use as VoIP.

The latest on the video bandwagon is the Skype 2.0 release. At only 15 frames per second and 40 to 75 kbps upload and download, Skype Video works well on a standard home DSL line or better. Other popular IM clients with video include Microsoft's Messenger and Yahoo Instant Messenger. AIM now offers video as well.

H.323-based IP videoconferencing systems have been available in hardware and software from many sources for almost a decade at this point, so there's no shortage of vendors in this space. And SIP video phones are available from many of these same vendors and from startup companies in the SIP space.