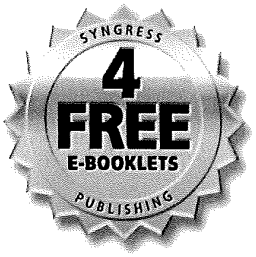
SYNGRESS®

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

Samsung Exhibit 1032

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

Are You 0wned?

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

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.