

## ***NEWS RELEASE***

**SecureLogix Contact:**

David Heard  
210-402-9669 (o)  
dheard@securelogix.com

**TippingPoint Contact:**

Kate Fly  
512-681-8218  
kfly@tippingpoint.com

### **McGraw-Hill Publishes “*Hacking Exposed: VoIP*” Book Co-authored by TippingPoint and SecureLogix Experts**

*Internationally Best-Selling Security Book Series Reveals  
VoIP Security Threats, Secrets and Solutions*

**AUSTIN, TX and SAN ANTONIO, TX, December 19, 2006** – TippingPoint and SecureLogix today announced the release of “*Hacking Exposed™ VoIP: Voice Over IP Security Secrets and Solutions*,” published by McGraw-Hill and co-authored by TippingPoint Director of Security Research David Endler and SecureLogix Chief Technology Officer Mark Collier.

This new book focuses on the specific threats to enterprise voice over IP (VoIP) networks, and is the latest addition to McGraw-Hill’s internationally best-selling *Hacking Exposed™* network security book series. The series aims to educate network security practitioners by detailing actual strategies, tactics, and weapons used by hackers to penetrate corporate data networks. A companion website with free security diagnostic tools can be found at [www.hackingvoip.com](http://www.hackingvoip.com).

As enterprise VoIP adoption continues to increase, so will the scope, frequency, and severity of VoIP-related network attacks. Although VoIP security has become a hot topic of discussion among voice administrators, the media, and industry analysts; little is really understood about which types of attacks are likely to be most prevalent, how these attacks will manifest, and what network administrators should do to prioritize and defend against these threats today and tomorrow.

***more...***

In conducting laboratory research for their book, Endler and Collier developed and demonstrated many real-world VoIP attack scenarios and tools that hackers will likely use to target enterprise VoIP deployments. "*Hacking Exposed:™ VoIP*" describes and ranks the various threats, pragmatically discusses which attacks are most likely to manifest over the coming months and years, and outlines how best to protect enterprise VoIP networks.

"Many of the existing discussions on VoIP security are a bit conceptual," explained Collier. "Our goal was to translate the theoretical into the practical, and give network administrators a real-world view into the tools and methods of a would-be VoIP hacker."

"Traditionally, the most prevalent threats to VoIP have been the same that have plagued data networks for years: worms, denial of service, and exploitation of the supporting infrastructure," said Endler. "Today, that is changing. As VoIP adoption continues to increase, hackers are also increasing their interest in VoIP technology. Consider last month's SANS Top 20 report that called out VoIP security issues as one of the most significant trends in 2006."

### **Book Reviews**

McGraw-Hill has obtained and published the following reviews of "*Hacking Exposed:™ VoIP*."

"The secret is out! Here is Zen and the art of hacking VoIP and making it secure. David and Mark write with a delightful enthusiasm that sustains this inside story on what it will take to make safe Internet telephony. Rich with concrete examples using open tools, many created by the authors, it's a must-read for everybody in modern communications engineering and management. It's also a fabulous book for any inquiring mind and the top of my recommendations this year."

-- Jonathan Zar, *Managing Director, Pingalo; Secretary and Outreach Chair, The VoIP Security Alliance*

"The authors do an excellent job of explaining possible security risks when companies move to VoIP. Of equal importance, the book describes countermeasures that can be deployed so that the potential of VoIP can be realized in a secure manner."

-- Gustavo de los Reyes, *Technical Consultant, AT&T*

"The VoIP-enabled phone conversations and conference calls you are participating in today are not as secure as you might think. This book illuminates how remote users can

probe, sniff, and modify your phones, phone switches, and networks that offer VoIP services. More importantly, the book offers solutions to mitigate the risk of deploying VoIP technologies."

-- Ron Gula, *CTO of Tenable Network Security, which produces the Nessus Vulnerability Scanner*

### **About David Endler**

David Endler is the director of security research for 3Com's security division, TippingPoint, where he leads 3Com's internal product security testing, VoIP Security Center, and TippingPoint's vulnerability research teams. Endler is also the Chairman of the Voice over IP Security Alliance (VOIPSA), founded by TippingPoint in 2005 and now with over 100 member organizations. Previously, Endler performed security research for Xerox Corporation, the National Security Agency, and MIT. Endler is the author of numerous security articles, and holds a Masters degree in Computer Science from Tulane University.

### **About Mark Collier**

Mark Collier is CTO of SecureLogix Corporation, an enterprise telephony management and security company. Mr. Collier is responsible for technology research, development, and related intellectual property, including a special focus on VoIP security solutions. He has completed publicly funded research into current and future threats to VoIP systems, protocols, and application services. Mr. Collier is a frequently quoted author and presenter on the topic of voice and VoIP security, and was recently named one of "The 50 Most Influential People in VoIP" by VoIPNews. Mr. Collier authors a popular blog discussing VoIP security issues at [www.voipsecurityblog.com](http://www.voipsecurityblog.com).

### **About TippingPoint, a division of 3Com**

TippingPoint, a division of 3Com (Nasdaq: COMS), is the leading provider of network-based intrusion prevention systems. The TippingPoint IPS is the most decorated in its industry. For a full list of awards, visit [http://www.tippingpoint.com/products\\_certifications.html](http://www.tippingpoint.com/products_certifications.html). Our innovative approach offers customers unmatched network-based security with ultra-high performance, scalability and reliability. TippingPoint is based in Austin, Texas, and can be contacted through its Web site at [www.tippingpoint.com](http://www.tippingpoint.com) or by telephone at 1-888-TRUE-IPS.

### **About SecureLogix**

SecureLogix, a Gartner designated "Cool Vendor" and a member of the *Deloitte Fast 500*, builds first-of-kind solutions that secure enterprise telecom resources from attack and abuse and simplify voice network management. SecureLogix® technologies are currently protecting and managing over two-and-a-half million phone lines for small-to-large commercial and government organizations.

###

SecureLogix, SecureLogix Corporation, and the SecureLogix Diamond Emblems are trademarks or registered trademarks of SecureLogix Corporation in the U.S.A. and other countries. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

U.S. Patents No. US 6,249,575 B1, US 6,320,948 B1, US 6,542,421 B2, US 6,687,353 B1, US 6,718,024 B1,  
US 6,735,291 B1, US 6,760,420 B2, US 6,700,964 B2, US 6,879,671 B2, US 7,133,511 B2, and CA 2,354,149.  
U.S. and Foreign Patents Pending.

Copyright © 2005 3Com Corporation. 3Com, and the 3Com logo are registered trademarks and TippingPoint is a trademark of 3Com Corporation or its subsidiaries. All other company and product names may be trademarks of their respective holders.