"This book gives you the knowledge you need to defend your Cisco-based network against the threats of today and tomorrow." —*From the foreword by Michael Lynn, Security Researcher and Black Hat Speaker*

HACKING Cisco® Networks™ EXPOSED

Cisco Security Secrets & Solutions

Dr. Andrew Vladimirov, Konstantin V. Gavrilenko,
Janis N. Vizulis, and Andrei A. Mikhailovsky

HACKING EXPOSED™ CISCO® NETWORKS: CISCO SECURITY SECRETS & SOLUTIONS

DR. ANDREW A. **VLADIMIROV**
KONSTANTIN V. **GAVRILENKO**
JANIS N. **VIZULIS**
ANDREI A. **MIKHAILOVSKY**

McGraw-Hill/Osborne
New York Chicago San Francisco
Lisbon London Madrid Mexico City
Milan New Delhi San Juan
Seoul Singapore Sydney Toronto

The McGraw-Hill Companies

McGraw-Hill/Osborne
2100 Powell Street, 10th Floor
Emeryville, California 94608
U.S.A.

To arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact **McGraw-Hill**/Osborne at the above address.

Hacking Exposed™ Cisco® Networks: Cisco Security Secrets & Solutions

1234567890 CUS CUS 0198765

ISBN 0-07-225917-5

Executive Editor
Jane K. Brownlow
Senior Project Editor
LeeAnn Pickrell
Acquisitions Coordinator
Jennifer Housh
Technical Editors
Wesley J. Noonan
Eric S. Seagren
Copy Editor
Lisa Theobald
Proofreader
Paul Tyler
Indexer
Karin Arrigoni
Composition and Illustration
Apollo Publishing Services
Series Design
Peter F. Hancik, Dick Schwartz
Cover Series Design
Dodie Shoemaker

This book was composed with Adobe® InDesign®

HACKING EXPOSED™ CISCO® NETWORKS: CISCO SECURITY SECRETS & SOLUTIONS

The authors would like to dedicate this book to the security community, as well as the open source and full disclosure movements.

About the Authors

Dr. Andrew A. Vladimirov

Dr. Andrew A. Vladimirov (Bristol, England), CCNP, CCDP, CISSP, CWNA, TIA Linux+, is a researcher with a wide area of expertise ranging from applied cryptography and network security to bioinformatics and neuroscience. He published his first scientific paper at the age of 13 and is one of the co-founders of Arhont Ltd., one of the leading IT/network security consultancies in the UK. Andrew has extensive experience working with Cisco routers, switches, and PIX firewalls, including design and penetration testing of Cisco-based networks, and has previously uncovered and published several flaws in IOS at Bugtraq. He has also published a variety of papers devoted to network/protocol security and authored a chapter on the subject of wireless security in *Network Security: The Complete Reference* (McGraw-Hill/Osborne) and is a co-author of *Wi-Foo: The Secrets of Wireless Hacking* (Addison Wesley, 2004). Andrew is supportive of both the open source and full disclosure movements. He is a graduate of Kings College London and the University of Bristol.

Konstantin V. Gavrilenko

Konstantin V. Gavrilenko (Bristol, England) has more than 12 years' experience in IT and security and together with his co-authors is a co-founder of Arhont Ltd. Konstantin's writing draws primarily from his real-world knowledge and experience in security consultancy and infrastructure development for a vast range of clients. He is open minded and enthusiastic about research, where his main areas of interest lie in security in general and more specifically in firewalling, cryptography, VPNs, and IDS. Konstantin has an extensive experience working with Cisco PIX firewalls and Cisco VPN concentrators and client applications. He is proud to say that he is an active supporter of open source solutions and ideology, public disclosure included. Konstantin has published a variety of advisories at SecurityFocus and PacketStorm, uncovering new software security vulnerabilities, along with being a co-author of the bestselling *Wi-Foo: The Secrets of Wireless Hacking*. He holds a first class BS honors degree in Management Science from DeMontfort University and an MS in Management from Lancaster University.

Janis N. Vizulis

Janis N. Vizulis (Bristol, England) is a researcher and programmer with a wide area of expertise ranging from digital forensics (11 years of forensics experience in criminal police work) to black and white box penetration testing with a main focus on the gambling industry, including security consultancy in the development of online banking applications for major players in the gambling industry and developing anti-DDoS and load-balancing solutions, many of them Cisco-based. His main interest in security lies in network protocols and web application security, including the development of

protocol and application fuzzing tools for new vulnerabilities discovery and equipment and application security stress-testing. Janis was the leading developer of the new tools released during the writing process of this *Hacking Exposed* tome.

Andrei A. Mikhailovsky

Andrei A. Mikhailovsky (Bristol, England) first became enticed by UNIX flavors back in school. He cultivated and expanded his knowledge into networking aspects of information technology while obtaining his bachelor's degree from the University of Kent at Canterbury. Soon he was engrossed in network security and penetration testing of Internet-centric equipment including various Cisco devices. On accomplishing his MBA, he co-founded information security company Arhont and participated in security research, published articles and advisories, and greatly contributed to the overall success of the Arhont team. Andrei's technical particularities include user authentication mechanisms, database and directory services, wireless networking security, and systems integration. He has extensive experience working with Cisco implementations of RADIUS and TACACS authentication protocols.

About the Technical Reviews

Wesley J. Noonan

Wesley J. Noonan (Houston, Texas) has been working in the computer industry since the mid-1990s, specializing in Windows-based networks and network infrastructure security design and implementation. He is a Staff Quality Engineer for NetIQ working on the company's security solutions product line. Wes is the author of *Hardening Network Infrastructure* and is a contributing/co-author for *The CISSP Training Guide* by QUE Publishing, *Hardening Network Infrastructure* (McGraw-Hill/Osborne), and *Firewall Fundamentals*. Wes is also a contributor to *Redmond* magazine, writing on the subjects of network infrastructure and security. He has presented at TechMentor 2004 and maintains a Windows Network Security–related "Ask the Experts" section for Techtarget.com (*http://searchwindowssecurity.techtarget.com/ateAnswers/0,289620,sid45_tax298206,00.html*).

Eric S. Seagren

Eric S. Seagren (Missouri City, Texas), CISA, CISSP-ISSAP, SCNP, CCNA, CNE, MCP+I, MCSE, has nine years of experience in the computer industry, with the last seven years spent in the financial services industry working for a Fortune 100 company. Eric started his computer career working on Novell servers and performing general network troubleshooting for a small Houston-based company. While working in the financial services industry, his duties have included server administration, disaster recovery responsibilities, business continuity coordinator, Y2K remediation, and network vulnerability assessment responsibilities. He has spent the last few years as an IT architect and risk analyst, designing and evaluating secure, scalable, and redundant networks.

FOREWORD

At the time of this writing, I am the only person to have publicly demonstrated the ability to reliably exploit buffer overflows on Cisco routers. Considering that we know others are looking to do the same thing, we don't have much time. We can either hope that when they find out how, they will be as open and helpful as I have tried to be, or we can prepare for the worst. Hope is not a defense strategy.

The ability to maliciously take control of a router or a switch is a much more serious compromise than an attack on a workstation or a server, because it gives the attacker a favorable network position. Routers are responsible for forwarding our traffic across the network, so attackers can listen to and modify all traffic being passed through the hacked device. This means that a router can become a spring board to compromise entire networks, all from a single device. A slightly more sophisticated attacker can use the fact that he or she is now in the middle of the traffic to perform attacks on encrypted networks. These man-in-the-middle attacks can allow hackers to decrypt virtual private networks and gain access to the data they protect.

Such exploitation has been the holy grail for many would-be attackers. The source code for Cisco's IOS has been stolen on at least two occasions. The only reason to steal this source code is to find vulnerabilities and create exploits to attack routers and switches. My research took more than six months of full time reverse-engineering work to demonstrate such an attack—with source code, this would have taken far less time and skill. We know that source code thieves are working on this, and it's doubtful they will come forward and do the right thing when they succeed.

The exploitation of security vulnerabilities in our routers and switches is bad enough, but that's just the beginning. The next threat will be worms that attack our network infrastructure. Unlike worms that attack endpoints, a network infrastructure attack could cripple the network in ways that are much more difficult to recover from. How do you ship a software fix when the infrastructure itself is down? The worst case scenario is an attacker gaining control of a router and erasing the boot instructions from a router's flash—effectively rendering the device unusable from then on. This makes for the gruesome possibility that malicious network traffic can actually destroy network hardware. Imagine how much that would cost your organization in lost equipment and down time?

Few network administrators would place an important server or workstation directly on the Internet without the protection of a firewall. Today, most border routers, the devices that connect intranets to the Internet, sit unprotected from malicious traffic. Most of us are unprepared to defend our intranet gateways against these new threats, and we may not even have a way to know whether we've been attacked.

A good admin regularly patches workstations and servers even when they are protected by firewalls. Routers and switches, on the other hand, often go overlooked in patching. While they are more important to the network infrastructure, it is not uncommon for our network devices to remain unpatched from the day they are installed to the day they are retired.

It's clear that a storm is brewing on the horizon, but the good news is that we still have time to prepare our defenses. We can do a number of things to ensure the continued security and operation of our networks, and the solution starts with the kinds of people buying this book.

Start with questioning any vendor's claims about security. It's clear now that no computer system can be totally secure, and any such claim should be met with suspicion. Sometimes vendors lie; don't be afraid to confront your vendor about security. It can take a year or more for a major network device vendor to release details about a security issue, and when they do disclose information they often downplay the issue to an extent that no one takes it seriously. When a vendor misleads you about the severity of an issue, they damage your ability to triage issues and ultimately reduce your ability to defend your network.

This is no longer acceptable.

For their part, vendors must fess up to the problems in their systems. We can't fix something if we can't agree that it is broken. All systems have bugs—what is important is how a vendor deals with the bugs in its products. It's no longer acceptable for a vendor to cover up a security issue rather than address the problems openly. As customers, it's your job to pressure vendors to do the right thing.

We have to start thinking of routers and switches as networked computers. They need to have proper patch management procedures that get fixes for issues as they happen. To the extent that it is practical, we need to firewall off our routers just as we would any other host. This will require that vendors take the process of patch management as seriously as network administrators do.

Responsible engineering practices dictate that any firmware-based system with modifiable images must have a reliable way to restore a system after an incident. Routers and switches should no longer be manufactured without fail-safe, hardware enforced read-only boot images. It's worth the extra 50-cent ROM chip to make sure your $20,000 router doesn't become a boat anchor.

We have survived attacks targeted at our all-Microsoft endpoints, but the stakes are much higher on our network devices. In the long-term ecology of networking, we must learn to resist homogeneity at the infrastructure level in order to survive. If we are going to combat network destroying worms and VPN spying exploits, we are going to have to start running a more diverse code base on our network devices. That means that vendor initiatives such as the Cisco powered network, which are designed to enforce network

monoculture, must be resisted. Conventional wisdom once held that routers and switches were not vulnerable to attack in the same way as our network endpoints. Consequently, most of our network infrastructure received about the same security attention as the toaster oven in the IT department break room. Today the revelation that Cisco's ubiquitous IOS operating system can be attacked by hackers, just like any other computer, renders conventional wisdom obsolete.

No network administrator should be without a solid understanding of the risks we face today. The *Hacking Exposed* series provides all the information you need to plan your defense with confidence. *Hacking Exposed Cisco Networks* continues that tradition by showing you step by step where the problems are and explaining in-depth how to solve them. This book gives you the knowledge you need to defend your Cisco-based network against the threats of today and tomorrow.

Consider this: it took Roger Bannister a lifetime of training to run the first 4-minute mile. It only took six months for someone else to follow. The clock is ticking. Have you started preparing your defense yet?

—Michael Lynn

Michael Lynn has an extensive background in embedded systems, including kernel development. His research interests include signals intelligence, cryptography, VoIP, reverse engineering, and breaking any protocol designed by committee. His current research focuses on securing critical routing infrastructures. He was the first person to demonstrate publicly that buffer overflows can be reliably exploited on Cisco routers and switches.

CASE STUDY: THE BLACK HAT HASSLE

At the Black Hat Briefings in Las Vegas, Nevada, on July 27, 2005, after Michael Lynn delivered his key presentation, "The Holy Grail: Cisco IOS Shellcode and Exploitation Techniques," a man with an impressive badge walked up to him and said: "I need to speak with you. Now." This is what happened next according to an interview with Michael that appeared in Wired News (*http://www.wired.com/news/privacy/0,1848,68365,00.html?tw=wn_tophead_1*):

> "There were a lot of flashy badges around from lots of three-letter agencies. So they take me to a maintenance area and I'm surrounded by people…and one of them says (to another guy), "You've got the van ready?" I'm going, "Oh my god." And they go, "Just kidding!... Oh, man, you rock! We can't thank you enough." And I'm just sitting there, like still pale white. They all shook my hand. I get the feeling that they were in the audience because they were told that there was a good chance that I was about to do something that would cause a serious problem. And when they realized that I was actually there to pretty much clue them in on…the storm that's coming…they just couldn't say enough nice things about me."

The story actually started long before the Black Hat conference. On January 26, 2005, Cisco announced a vulnerability called "Multiple Crafted IPv6 Packets Cause Router Reload." The next day, after a night of research, Lynn already knew that this flaw could lead to much more than forcing the router to reload. It could lead to enable. Cisco did not believe him, though and, according to Lynn's interview, Cisco higher-ups told him that he was lying. They also refused to provide any information to Internet Security Systems (ISS), for which Lynn worked at the time.

This reply seemed particularly strange, since research by the Phenoelit group had already demonstrated the feasibility of IOS exploitation techniques, and three proof-of-concept exploits for this system were already available to the general public for years.

In an interview with FX that appeared on the SecurityFocus web site *http://www.securityfocus.com/columnists/351*, FX told the columnist that *he* had completed the first IOS exploit by the end of 2001. When the columnist mentioned to FX that, "Now a lot of people want to be the first to reach the goal: make public some working shellcode," FX's reply was "Really? They should come out and talk to me." However, FX did get a full credit in Lynn's Black Hat presentation, and statements about "the first IOS exploitation technique ever" stem entirely from the press's incompetence.

In the meantime, ISS management, dissatisfied with Cisco's response, asked Lynn to disassemble the IOS to find out more about this particular vulnerability. Since we don't know which agreements existed between Cisco and ISS at the time, we can't judge whether such a request was legitimate. But Lynn had to spend months reverse-engineering IOS until this serious flaw was fully researched and described. Cisco engineers still did not believe that the exploitation was possible, however. To prove that the claim was not just hot air, ISS managers invited one of the IOS architects to Atlanta to demonstrate the flaw. He arrived on June 14, 2005, and was impressed by what he saw. Lynn describes this as the day when Cisco found out about the nature of his work and the content of his presentation-to-be—more than a month before the Black Hat Briefings took place.

Initially, Cisco representatives did not believe that the data Lynn had obtained would be presented to the public. Apparently, Lynn was against the exploit code distribution, fearing that the code would leak to crackers. However, ISS management was determined to bring the presentation forward, no matter what the impact. They also wanted to distribute a working exploit within the ISS, so that their sales and security engineers could benefit from it. Just a week before the presentation, ISS managers completely changed their minds and asked Lynn to withdraw the talk and present a lecture on VoIP security instead. They claimed that this request was made with no pressure from Cisco at all. In reality, however, Cisco had asked ISS to wait for a year to release the exploit and threatened a lawsuit against both Lynn and Black Hat organizers. Organizers were forced to allow Cisco representatives to tear out the pages with Lynn's work from the conference book. Two days before the talk, temporary workers hired by the company spent eight hours ripping out the pages (a process that was filmed and is available for download from the Internet).

All these events prompted Lynn to agree not to proceed with the presentation. However, he resigned from ISS two hours before the presentation and went forward with the talk anyway. He stepped onto the stage in a white hat with *Good* written on it. Lynn was introduced as speaking on a different topic, which elicited boos. But those turned to cheers when he asked, "Who wants to hear about Cisco?" As he started, Lynn said, 'What I just did means I'm about to get sued by Cisco and ISS." At the end of the talk, he asked the audience to look over his resume, wondering whether anyone had a job available for him. He told the audience that he had quit his job with ISS to give this presentation "because ISS and Cisco would rather the world be at risk, I guess. They had to do what's right for their shareholders; I understand that. But I figured I needed to do what's right for the country and for the national critical infrastructure."

Cisco made its own turn the same day by filing a request for a temporary restraining order against Lynn and the Black Hat organizers to prevent "further disclosing proprietary information belonging to Cisco and ISS," as John Noh, a Cisco spokesman, stated. In a release after the talk, a Cisco representative stated: "It is important to note that the information Lynn presented was not a disclosure of a new vulnerability or a flaw with Cisco IOS software. Lynn's research explores possible ways to expand exploitations of known security vulnerabilities impacting routers." As you will see, this statement is true. At the same time, the Black Hat Briefings organizer and founder Jeff Moss denied that he had any idea of Lynn's intent to present the IOS exploitation data instead of giving the backup talk about VoIP.

With the help of Jennifer Granick, Lynn's legal representative, the lawsuit has been settled. Lynn and the Black Hat organizers had to agree to a permanent injunction barring them from further discussing the now infamous presentation. The injunction also requires that Lynn return any materials and disassembled IOS code. He is also forbidden from making further presentations at the Black Hat or the following Defcon 13 hacker conference. In addition, Lynn and Black Hat agreed never to disseminate a video made of Lynn's presentation and to deliver to Cisco any video recording made of it. Despite this agreement, the FBI launched an investigation and, at the moment of writing this case study, its outcome is unclear.

Cisco has produced a security advisory stating that an arbitrary code execution from a local network segment using the methodology described at the Black Hat presentation is possible. This advisory, released on July 29, 2005, is called "IPv6 Crafted Packet Vulnerability" and, as it should do, contains a long list of fixes for the problem. You can view the advisory at *http://www.cisco.com/en/US/products/products_security_advisory09186a00804d82c9.shtml*. The fixes require a full IOS upgrade, and no temporary workaround is available other than not using IPv6 on the affected routers.

Meanwhile, copies of Lynn's presentation have spread all over the Internet—some complete and some with partially blacked-out code. Pictures of the original slides are hosted at foreign sites. ISS has tried to silence some of the sites with the presentation-related materials, and its attorneys sent out cease-and-desist letters to the sites' owners. However, this did not stop the data from dissemination, and by now we would assume that any security expert or hacker interested in the topic has seen it. Multiple articles appeared in the news—in both general and technical media—about the case. Hardly any of them can be called *impartial*, however, as some clearly sided with Lynn, some with Cisco and ISS, and some with both.

We are not experts on ethics; neither do we want to enforce our opinions on the readers. Thus, we leave the moral judgement on these events open to your own discretion. As to the technical side of the question, our take on the IOS exploitation approaches is reflected in Chapters 8 and 10 of this book.

ACKNOWLEDGMENTS

The existence of this book would not have been possible without the support, help, and understanding of many people and organizations. First of all, we acknowledge the valuable assistance and collaborative support provided to us by the team of McGraw-Hill/Osborne editors, including executive editor Jane Brownlow, acquisitions coordinator Jenni Housh, senior project editor Lee Ann Pickrell, and editor Lisa Theobald. The deepest thanks goes to Boris Chernov for his perfect technical assistance in the matters of software engineering and the overall help with this book. A lot of things were corrected and improved due to the vital contribution of Wes Noonan, our main technical editor. We are also grateful to FX for the initial help with technical edits and everyone in the Phenoelit team for their ingenious contribution to IOS security research. Thanks also goes to Michael Lynn for his work and presentation on Cisco IOS internals and potential exploitation. Last, but not the least, we are grateful to James Blake for donating some equipment for our testing lab. Keep up the good work and again many thanks for all the help, contributions, and support that we've received in the course of writing this book.

INTRODUCTION

Perhaps the real difference between the Jedi and the Sith lies only in their orientation; a Jedi gains power through understanding, and a Sith gains understanding through power.

—Darth Sidious

THE PECULIARITIES AND HARDSHIPS OF CISCO-RELATED ATTACKS AND DEFENSES

Some *hackers* (in a loose meaning of this battered term) try to understand everything about the internal workings of a system or protocol they have targeted, and only then do they begin the exploitation. Others try to break it using all means at their disposal and learn about the system in the process of breaking it. The methodologies we describe in this book can appeal to the followers of both paths. At the end of the day, it is the results that count, and an approach that works best for the attacker would be embraced by him or her as true. In our specific case, the result is usually called *enable*.

An attacker who goes after Cisco networking devices can be a CCIE Security consultant, performing a legitimate security audit. He can be a renegade system programmer, armed with disassembly tools and searching for great fame or equally great stealth. She might be an experienced network engineer with an arsenal of powerful sniffing and custom packet generating utilities and a craving for the takeover of the whole network via an unknown glitch in a proprietary protocol design. Or, perhaps a novice hacker has just discovered what really runs the modern Internet and wants to experiment with these mysterious and powerful hosts. As the person responsible for the security of a network, you have to be ready to cope with all types of attackers and everything they can throw at the target. As a security auditor, you have to be capable of emulating all kinds of attackers, understanding their mentality, approaches, methods, and techniques. Only by starting the audit while behaving like the lowest denominator of cracker, and ending it acting like a highly professional Black Hat, can a penetration tester do a proper external or internal risk assessment of the audited network.

This is not easy. First of all, everything related to Cisco systems and protocols hacking is only beginning to emerge from the shadows. You won't find a lot of comprehensive information about this online, and this book is the world's first printed literature source entirely devoted to this issue. Another difficulty you (and the attackers) will inevitably encounter is the great variety of Cisco devices and versions of the operating systems that they run—routers, switches, firewalls, VPN concentrators, IDS sensors, wireless access points, and so on. They run various versions of IOS, CatOS, PIX OS, and even general purpose operating systems such as Solaris and Linux. To make things more difficult, many OS versions are specifically bound to the hardware they run on for efficiency and optimization reasons. This is particularly important for a highly skilled attacker trying to write a shellcode for his exploit.

When Next Generation (NG) IOS appears and good old CatOS eventually dies out, truly cross-platform exploits for Cisco routers and switches may become possible. For now, an exploit will work against a specific platform only, and a hacker would need to spare some time and effort to find offset addresses for different IOS versions running on that particular platform. It should be noted that network administrators in general seem to be somewhat conservative and not truly eager to update the operating systems of their routers and switches. We have encountered many cases of IOS 11.X and CatOS 4.X still running on the audited hosts. Thus, older IOS and CatOS versions are here to stay for quite a while, even after the much talked about IOS NG is released.

On the defenders' side, the differences between the system versions mean that some countermeasures will be available on the systems you control, and some won't. Moreover, the same safeguard could be configured on distinct system versions using different commands or variations of the same command. This makes the device and the overall network defense a rather complicated task. A lot of material, mostly from Cisco itself, has been released on the subject of securing Cisco devices and whole networks, but blindly typing the commands mentioned in the manual does not help the administrator to understand the full impact or implications of the attack these commands may prevent. Thus, the incentive to spend time on thoroughly configuring existing security features and patching the known flaws may run very low. What is needed is an all-around Cisco security resource, providing a professional description and systematic balanced approach to both attack and defense. We have strived to adhere to this requirement as much as possible and hope that this book will meet at least some of your expectations.

We have also tried to dispel common mythology surrounding the peculiarities of Cisco device and network security and halting the development of this important information security field. The harmful myths currently circulating within the world security community, from corporate security managers to lowly script kiddies, are many and include the following:

- Cisco routers, switches, PIX firewalls, and so on are secure by default and can't really be broken into, unless they are badly misconfigured.
- To the contrary, Cisco routers are very easy to break into (this opinion is common among the "Telnet password and SNMP community guessing crowd," a part of the "hooded yob" populating so-called "underground channels").

- Running the IOS privileged EXEC mode `auto secure no-interact` command will automatically sort out all your security headaches, even if you don't know much about router security.
- The cracking underground is not really familiar with Cisco network appliances and rarely selects them as targets.
- There is little the intruders can do with a taken over Cisco router and nothing they can do with an "owned" Catalyst switch. At worst, they will erase both Flash and NVRAM.
- An intruder cannot preserve his access to an owned Cisco router or other device without leaving telltale signs in its configuration file.
- Data link layer attacks are for weirdoes. You can do the same things with ARP spoofing, right?
- Crackers can bring down the whole Internet via a BGP-based attack, and it is easy to do.
- To the contrary, BGP is completely secure and unbreakable. Proprietary routing protocols are also very secure, since their full specifications are not known to attackers.
- Buffer overflow attacks against IOS are impractical and too difficult to execute. Writing exploits against this system is an extreme form of rocket science, known only to the few remaining Illuminati.
- Patching the IOS binary image to inject malicious code is also next to impossible. Such an image won't be accepted by the router or won't function properly.
- Attacking another router from (not through!) a hacked router? That's impossible! Cisco cross-platform worm? You must be joking!

Whether you prefer to gain power through understanding or understanding through power, we hope that the contents of this book will convince you that these statements are, to put it politely, rather economical with the truth, which often lies somewhere in the middle.

ALL THE POWER OF HACKING EXPOSED AND MORE

This tome is written in the best tradition of the *Hacking Exposed* series. However, we've included a few differences, such as the way risk ratings are handled.

The topic of Cisco-related hacking isn't exactly the most researched topic. Many potential security threats and attack algorithms described here are little-known or new and were discovered during the process of writing this book. To do this, we assembled a tiny testing and research Cisco network, consisting of three 2500 and two 2600 series routers, Catalyst 2950 and 5000 series switches, PIX 515E and PIX 501 firewalls, a 3000 series VPN concentrator, and an Aironet 1200 wireless access point. We have also employed a couple of Gentoo and Debian Linux machines running Quagga and various attack and network monitoring/analysis tools mentioned through the book. A maximum