SECURE
COMPUTING

internet SECURITY

Special Black Hat Briefings '98 Issue

Up-to-the-minute news on computer security threats

It's late. You're in the office alone, catching up on database administration. Behind you, your network servers hum along quietly, reliably. Life is good. No one can get to your data or disrupt your WAN.

The network is secure. Or is it?

Black Hat Briefings '98 has been organized to put an end to concerns like these. While many conferences focus on information and network security, only Black Hat Briefings '98 will put your engineers and software programmers face-to-face with today's cutting edge computer security experts and "underground" security specialists.

Only the Black Hat Briefings will provide your people with the tools and understanding they need to thwart those lurking in the shadows of your firewall.

The reality is, they are out there.

The choice is yours.

You can live in fear of them.

Or, you can learn from them.

with compliments

CONTENTS

**We welcome your comments!
Please e-mail us at:**

Internet_Security@securecomputing.com

Available on-line at:

www.securecomputing.com/UpComing.html

Why Black Hat Briefings '98?

Conference Overview

Black Hat Briefings was created to fill the growing need of computer professionals to better understand the security risks threatening their computer and information infrastructures. To accomplish this, we assemble a group of vendor-neutral security professionals and invite them to talk candidly about the problems businesses face, and the solutions to those problems. No gimmicks, just straight talk by people who make it their business to explore the ever changing security space.

Spanning two days with two separate tracks, Black Hat Briefings '98 will focus on the vital security issues facing organizations with large enterprise networks and mixed network operating systems. Topics will include Intrusion Detection Systems (IDS), denial of service attacks and responses, secure programming techniques, and tool selection for creating and effectively monitoring secure networks.

Intense sessions will bring to light the security and misconfiguration problems confronting organizations and network administrators, most of which go unnoticed by today's preoccupied system administrators where security gets put off in lieu of constant network growth and upgrades. Experts will discuss the strategies involved in correcting existing problems and problems on the horizon.

Current Intrusion Detection Systems as well as methods of proactive prevention will be discussed with the intent of educating attendees on how to stop these problems before they occur. Chief Information Officers (CIO's) are welcome, as are the people implementing network strategies and building applications. The conference is designed for both policy maker and policy implementor.

The Premier Sponsor of Black Hat Briefings '98 is

SECURE
COMPUTING
Nobody Comes Close.™

Conference Agenda

Track A will be more general, Track B more technical.

Wednesday, July 29th

08:30 - 09:00 - Breakfast

09:00 - 09:45

Keynote Address: - Marcus Ranum - *How to REALLY secure the Internet*

10:00 - 11:30

Track A - Richard Thieme - Convergence - *Every man (and woman) a spy*

Track B - Dominique Brezinski - *Penetrating NT networks through information leaks and policy weaknesses*

11:40 - 13:10

Track A - Ira Winkler - *Information security: beyond the hype*

Track B - Theo DeRaadt - *A discussion of secure coding issues, problems with maintaining OS source trees, and secure program design philosophies*

13:20 - 14:20 - Lunch

14:25 - 15:20

Track A - Ray Kaplan - *Meet the enemy session*

Track B - Paul McNabb - *The use of trusted operating systems technology*

15:30 - 17:00

Track A - Bruce K. Marshall - *Statistical analysis of reusable password systems and their alternatives*

Track B - Scott Waddell - *Security Posture Assessment methodology*

Thursday, July 30th

08:30 - 09:00 - Breakfast

09:00 - 09:45

Keynote Address - Bruce Schneier - *Mistakes and blunders: A hacker looks at cryptography*

10:00 - 11:30

Track A - Patrick Richard - *Open network PKI design issues or "Business as Usual"*

Track B - Dr. Mudge - *Problems with VPN technologies*

11:40 - 13:10

Track A - Jennifer Granick - *What's different about evidence in computer crime litigation*

Track B - Peter Shipley - *An overview of a TCP/IP internals and its security strengths and weaknesses*

13:20 - 14:20 - Lunch

14:25 - 15:50

Track A - Winn Schwartau - *Introducing the time based security model and applying military strategies to network and infrastructural securities. (A/K/A Humbug)*

Track B - Tom Ptacek - *Problems with intrusion detection systems*

16:00 - 17:00

Panel Discussion One - The benefits and problems of commercial security software.

Panel Discussion Two- The merits of intrusion testing.

Closing

Speakers of Black Hat Briefings ‘98

Secure Computing Corporation, the premier sponsor of Black Hat Briefings ‘98, and DefCon Productions are pleased to announce the following Industry talents as featured speakers. These speakers will offer deep insight into the real security issues facing your network with no vendor pitches.

Note: Sessions will be technically oriented and last approximately one and a half hours each. The goal of the presentations is to inform the audience of current system vulnerabilities and fixes as well as future areas of concern.

Keynote Speaker - Marcus Ranum - President and CEO of Network Flight Recorder, Inc.

How to REALLY secure the Internet

Is it possible to really secure the Internet? With current technology and methods, the answer would appear to be a resounding “no.” We've tried security through stepwise refinement and security through consensus - the best remaining solutions are totalitarian and draconian. Mr. Ranum will present an outline for how the Internet could be secured through some simple, cost effective methods. He will also explain why this *will not* happen.

Marcus Ranum is CEO of Network Flight Recorder, Incorporated, and has been specializing in Internet security since he built the first commercial firewall product in 1989. He has acted as chief architect and implementor of several notable security systems including the TIS firewall toolkit and TIS Gauntlet firewall, whitehouse.gov, and the Network Flight Recorder. Marcus frequently lectures on Internet security issues, and is co-author of the “*Web Site Security Sourcebook*” with Avi Rubin and Dan Geer, published by John Wiley and Sons.

Keynote Speaker - Bruce Schneier - President of Counterpane Systems and author of *Applied Cryptography*

Mistakes and blunders: A hacker looks at cryptography

From encryption and digital signatures to electronic commerce and secure voting, cryptography has become the enabling technology that allows us to take existing business and social constructs and move them to computer networks. But unfortunately, a lot of cryptography is defective, and the problem with defective cryptography is that it looks just like good cryptography; most people cannot tell the difference.

Security is a chain that is only as strong as its weakest link. In his discussion, Mr. Schneier examines some of the common mistakes companies make when implementing cryptography, and also advises on how to avoid them.

Bruce Schneier is president of Counterpane Systems, the author of *Applied Cryptography*, and the inventor of the Blowfish algorithm. He serves on the board of the International Association for Cryptologic Research and the Electronic Privacy Information Center. He is a contributing editor to Dr. Dobb's Journal, and a frequent writer and lecturer on cryptography.

Theo DeRaadt - lead developer of OpenBSD

A discussion of secure coding issues, problems with maintaining OS source trees, and secure program design philosophies

Theo De Raadt heads the OpenBSD project. This 4.4BSD derived operating system project has increasingly placed its focus on the discovery and repair of security vulnerabilities. Due to a two year auditing process by a ten member team, OpenBSD is probably the most secure operating system in use today. For more information, visit:

http://www.OpenBSD.org/security.html

Ira Winkler - President of the Information Security Advisory Group

Information security: Beyond the hype

If you read the headlines today, you would think that no matter what people are doing to secure their networks, they will never be secure. This theory is widely accepted because the media focuses on the threats and stories about unstoppable geniuses that compromise even the Pentagon. The truth is that you can protect yourself from even the most diabolical genius.

This presentation discusses Information Security from a risk-based perspective. Yes, the threats to your systems are discussed, but more importantly, the vulnerabilities that actually allow the threats to compromise your systems are discussed. Using this information, you can implement the countermeasures needed to protect yourself and your organization. While there is no such thing as perfect security, you can protect yourself from the most serious threats. Mr. Winkler will also advise attendees on how to spend limited funding in the most efficient manner.

Ira Winkler, CISSP is considered one of the world's leading experts on Information Security, Information Warfare, information related crimes, and Industrial Espionage. He is author of the book, *Corporate Espionage*, and President of the Information Security Advisors Group. His clients include some of the largest companies and banks in the world. He is also a columnist for ZDTV with his column *Spy Files.* Previously, Mr. Winkler was with the National Security Agency (NSA) and was the Director of Technology at the National Computer Security Association (NCSA). He has also performed studies on Information Warfare for the Joint Chiefs of Staff.

Dominique Brezinski - Network Security Professional, Secure Computing Corporation

Penetrating NT networks through information leaks and policy weaknesses.

The focus of this presentation will be a demonstration of how Windows NT hosts can be queried for information and how that information can be correlated to provide an attacker with a path of least resistance. Even though many Windows NT networks have only a few remotely exploitable technical vulnerabilities (buffer over-runs, flawed CGI scripts, address-based

See Speakers *on page 4.*

Speakers *from page 3.*

authentication, and so on), most NT networks give away too much information. By analyzing the information, it is easy to find policy weaknesses that can be exploited to gain access to NT hosts. In his presentation, Mr. Brezinski will use custom tools to demonstrate these techniques on a small network.

Dominique Brezinski is a Network Security Professional at Secure Computing Corporation and has been concentrating on Windows NT and TCP/IP network security issues for four years. Prior to working for Secure Computing, Mr. Brezinski worked as a Research Engineer at Internet Security Systems where he was responsible for finding new vulnerabilities and security assessment techniques for Windows NT.

In 1996 Mr. Brezinski published a white paper entitled *"A Weakness in CIFS Authentication"* which revealed a serious flaw in the authentication protocol used in Windows NT (NT LM Security). His discovery demonstrated how an attacker could completely subvert the network authentication in Windows NT and gain unauthorized access to Windows NT servers. Mr. Brezinski has continued to demonstrate advanced techniques for assessing the risks present in Windows NT networks.

Richard Thieme - Thiemeworks, Inc.

Convergence —Every man (and woman) a spy.

Arbitrary digital interfaces — television, PCs, and PDAs — are converging, but that is only part of the story. The roles people play in work and life are converging too. Intelligence agents, knowledge managers for global corporations, competitive business intelligence agents, system administrators, hackers, journalists, and CIOs are becoming indistinguishable. Why does this matter? Because the ability to synthesize and integrate information, manage complexity and ambiguity, morph continually into roles appropriate to a shifting work context, and somehow remember who you are definitely matters! Our presentations of ourselves are the powerful levers for moving mountains in the digital world. Richard Thieme discusses why, and how, to do it.

Richard Thieme is a business consultant, writer, and professional speaker focused on the human dimension of technology and the work place. His creative use of the Internet to reach global markets has earned accolades around the world.

Thieme's articles are published around the world and translated into German, Chinese, Japanese, and Indonesian. His weekly column, *"Islands in the Clickstream,"* is published by the Business Times of Singapore, Convergence (Toronto), and South Africa Computer Magazine as well as distributed to subscribers in 52 countries. Recent clients include: Arthur Andersen; Strong Capital Management; System Planning Corporation; UOP; Wisconsin Power and Light; Firstar Bank; Northwestern Mutual Life Insurance Co.; W. H. Brady Company; Allstate Insurance; Intelligent Marketing; and the FBI.

Ray Kaplan - Network Security Professional Secure Computing Corporation

Who are the enemies of computer and network security?

Generally, "hackers" are regarded as criminals by the "legitimate community." Who are these "hackers" that continue to whack on our systems and networks? Are they just a bunch of delinquents devoid of morals, ethics, and common sense or can we learn from them? This session is intended to introduce the two sides of the security equation in a forum which fosters open, detailed, and honest communication.

While in the minority of reported computer crime statistics, the skilled outsider still represents a significant threat. This session explores who those outsiders are, their attitudes and techniques, as well as their successes and failures from the perspective of what we can learn from them to better protect our systems and networks. This classic session allows you to interact directly with members of the computer underground. Join us for some stimulating conversation with those who computer security professionals consider to be their enemies. Bring your questions.

Mr. Kaplan has been actively involved with system and network security as a consultant for over half of his more than 20 years in the industry. There is no question that he hacks. However, he is not a criminal. His clients have included the world's largest financial institution, smallest commodities broker, multinational and Fortune 100 companies from all segments of the economy, and public institutions all over the world.

Mr. Kaplan consults, lectures and teaches technical system and network related topics all over the world. His articles are frequently published in major computer journals and magazines. In over ten years of public speaking he has given over 2,000 technical, tutorial-style presentations and lectures. As a frustrated inventor, he is forever trying to rid the world of inefficiency, frustration and waste by pursuing new paradigms in the delivery of training, education and technical information.

Peter Shipley - Manager KPMG, Electronic Commerce Division

An overview of a TCP/IP internals and its security strengths and weaknesses.

Mr. Shipley's presentation discusses many currently popular Internet Network based attacks and how you can protect your site from such attacks. Common denial of service attacks will also be discussed, including those relating to the World Wide Web (WWW) and various buffer overflow attacks. Teardrop, Land, IP Spoofing, Smurf Attacks, Route-Redirections, and others will be covered as well.

Mr. Shipley is an independent consultant in the San Francisco Bay Area with nearly thirteen years experience in the computer security field. Mr. Shipley is one of the few individuals who is well known and respected in the professional world as well as the underground and hacker community. He has extensive experience in system and network security as well as programming and project design. Mr. Shipley's specialties

See Speakers *on page 5.*

Speakers *from page 4.*

are third party penetration testing and firewall review, computer risk assessment, and security training. He also performs post intrusion analysis as well as expert witness testimony. Mr. Shipley is currently concentrating his efforts on completing several research projects.

Scott Waddell - Cisco WheelGroup Corporation

Security Posture Assessment methodology

Security Posture Assessment methodology will be discussed in the context of a real-world example that highlights the pitfalls of point solutions to enterprise security problems. The second half of the presentation will cover the incident control and recovery process with examples of simple techniques that can assist in system forensics.

Scott Waddell served on the Countermeasures Engineering Team at the Air Force Information Warfare Center for four years before leaving the military to join WheelGroup Corporation in 1996. As co-founder of WheelGroup, he directed field engineering teams in conducting enterprise-wide Security Posture Assessments with the automated tool suite he co-authored for those consulting engagements. Those tools lead to the development of NetSonar, WheelGroup's network mapping and vulnerability analysis product, which was released shortly before Cisco Systems acquired WheelGroup in March, 1998.

Scott is currently working with the Cisco IOS Technology group in Austin, TX, as a network security research engineer.

Dr. Mudge - L0pht Heavy Industries System Administrator

Real world VPN implementation security issues

As one of the prominent members of the hacker group 'The L0pht', Mudge has been responsible for numerous advisories and tools in use in both the black hat and white hat communities. L0phtcrack, the Windows NT password decryptor, monkey, the S/Key password cracker, Solaris getopt() root vulnerability, sendmail 8.7.5 root vulnerability, Kerberos 4 cracker, and SecurID vulnerabilities are some of the recent offerings that Mudge has contributed to the security community.

Mudge recently finished cryptanalysis work with some of the top US cryptographers. The BBC, Wired Magazine, Byte Magazine, and the Washington Post have all covered Mudge and the L0pht's ongoing projects.

Jennifer Granick - Attorney at Law

What's different about evidence in computer crime litigation

Solving and prosecuting computer crimes requires evidence. But electronic footprints, signatures and trails raise questions of preservation,verification and authenticity that their analog counterparts do not. This presentation will look at what is different about evidence in computer crime litigation, and how to properly preserve and maintain electronic evidence for law enforcement and prosecutors.

Jennifer Stisa Granick is a criminal defense attorney in San Francisco, California. She defends people charged with computer related crimes, as well as other offenses. Jennifer has been published in Wired and the Magazine for the National Association of Criminal Defense Lawyers.

Thomas Ptacek - Network Security Professional at Secure Networks, Inc.

Defeating Network Intrusion Detection

Network Intrusion Detection (ID), a technology that attempts to identify attackers by monitoring network traffic, is becoming one of the hottest products in the security market. But beneath the hype, lie some serious concerns about the reliability of ID systems and the fundamental techniques they use to collect information. This talk will explain why the most popular ID systems on the market cannot be trusted. Mr. Ptacek will also demonstrate how to avoid detection by them, and in the process, eliminate some widespread misunderstandings about the capabilities of sniffers and intrusion detection systems.

Thomas Ptacek is a developer at Secure Networks, Inc. His work focuses on vulnerability assessment, which involves researching and testing network systems for exploitable design and implementation flaws. In the course of this work, his team has discovered some of the Internet's most serious security problems, including vulnerabilities in Windows NT, Checkpoint Firewall-1, and Solaris, as well as core Internet software such as BIND, INN, and Apache.

Patrick Richard - CIO Xcert Software Inc.

Open network PKI design issues or "Business as Usual"

Co-founder of Xcert Software Inc. and Chairman and Chief Technology Officer, Mr. Richard is chief architect of the Xcert Universal Database API (XUDA) and leads Xcert's core development team. While a co-op student studying Mathematics and Computer Science at the University of Waterloo, Mr. Richard worked on distributed messaging technologies at Northern Telecom and Microsoft. In 1994 Mr. Richard founded Whistler Networks, the first true "virtual community" in British Columbia.

Mr. Richard has pioneered the integration of strong cryptography with distributed databases on the Internet. He established the first web-based certificate authority (CA) on the Internet and created the first public website that used client authentication using digital certificates. Mr. Richard is an active member of several related IETF working groups, including PKIX, CAT, TLS and ASID, and is the author of several papers on cross-authentication technology.

Bruce K. Marshall - CISSP at Feist Communications

Statistical analysis of reusable passwords and recommendations

Mr. Marshall's presentation focuses on an analysis of the passwords of 3,163 users of a corporate computer network. Using actual user passwords from a

See Speakers *on page 6*.

Speakers *from page 5.*

project Feist initiated, he was able to input them into a database and search for information and correlations. Mr. Marshall will use this data along with data from a similar study conducted in 1979 to show some time and trend progressions. The results will not shock any of us who have dealt with security and know reusable passwords are insecure, but it will provide hard figures and new analysis.

Bruce K. Marshall is an Information Security Specialist for Feist Communications Inc. He has studied identification and authentication systems for several years to gain insight into their inherent strengths and flaws. While the world grows increasingly computer based, he has fought to enforce acceptable means of securing these systems. As a member of the Biometric Consortium and other security groups, Bruce has been exposed to a wide variety of alternatives to standard authentication methods.

Paul McNabb - CTO of Argus Systems Group, Inc.

The use of trusted operating systems technology

The focus of this presentation will be the use of trusted operating systems technology to solve today's security problems with a particular focus on enabling electronic commerce.

Paul McNabb is the CTO of Argus Systems Group, Inc. and has been involved in developing trusted operating systems for the last ten years and has been developing low level UNIX software for the last eighteen years. Paul McNabb is one of the world's leading authorities on trusted operating systems.

Winn Schwartau - President of Interpac, Inc. and author of *"Chaos on the Electronic Superhighway" Information Warfare*

Introducing the Time Based Security model and applying military strategies to network and infrastructural securities.

Trivia bytes

What is so important about protecting data on the Internet? After all, how many people is the Internet really reaching? These facts speak for themselves, proving that the Internet is indeed going where no medium has gone before.

According to the US Commerce Department, three million people were connected to the Internet in 1994. By the end of 1997, that number had grown to 100 million. Internet traffic doubles every 100 days.

The San Francisco Examiner reported that the Internet is growing faster than all other media technologies that proceeded it. To reach an audience of a 50 million people, it took radio 38 years, television 13 years, and the Internet only four years.

Unfortunately, along with the rapid growth of the Internet came a little thing called *spam*. The New York Times and Associated Press reported that the number of unsolicited email ads sent per day by Cyber Promotions via the Earthlink network soared as high as 25 million. Cyber Promotions later paid Earthlink two million dollars to settle an "anti-spamming" lawsuit. As they say, you have to learn to take the good with the bad.

Looking back: Black Hat 1997

The first annual Black Hat Conference was a tremendous success, but you don't have to take our word for it, see for yourself. Links to the transcripts of speeches given at the 1997 conference, as well as digitized downloads , and speaker bios are available at :

http://www.blackhat.com/html/speakers.html

The 1997 conference also caught the attention of the media. Check out the following links to Black Hat Briefings 1997 media mentions:

The rise of the underground engineer

http://www.blackhat.com/html/blackhat-eetimes.html

The good bad guys vs. the bad bad guys

http://techweb.cmp.com/eet/whitepaper/paper1/paper1c.html

Warnings for an electronic nation

http://techweb.cmp.com/eet/whitepaper/paper1/paper1c.html

Humble pie

http://www.blackhat.com/html/black-hat-eetimes-2.html

Microsoft opens dialogue with NT hackers

http://www.blackhat.com/html/black-hat-eetimes-3.html

Registration Information

If you are interested in attending the Black Hat Briefings Conference 1998, registration costs are $995 US before July 10th 1998. Late registration fees are $1,195 after July 10th. This includes two days of speaking, materials, three meals on Wed., two meals on Thursday and a reception.

You may register for the Black Hat Briefings 1998 at the following Web site:

http://www.blackhat.com/html/nss-index.html