SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

Syngress Force 2006

Emerging Threat Analysis

FROM MISCHIEF TO MALICIOUS

A One-Stop Reference Containing the Most Read Topics in the Syngress Security Library

David Maynor
Lance James
Spammer-X
Tony Bradley
Frank Thornton
Brad Haines
Brian Baskin
Hersh Bhargava
Jeremy Faircloth
Craig Edwards
Michael Gregg
Ron Bandes
Anand M. Das
Paul Piccard

FEATURING DAVE MAYNOR'S DEVICE DRIVER RESEARCH THAT ROCKED BLACK HAT VEGAS!

FOREWORD BY DAVID MAYNOR
SENIOR RESEARCHER, SECUREWORKS

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE
To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of value-added features such as free e-booklets related to the topic of this book, URLs of related Web site, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs
Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS
For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET
Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING
Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING
Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

SYNGRESS®

Syngress Force

Emerging Threat Analysis

FROM MISCHIEF TO MALICIOUS

David Maynor
Lance James
Spammer-X
Tony Bradley
Frank Thornton
Brad Haines
Brian Baskin
Thomas Porter
Anand M. Das
Hersh Bhargava
Jeremy Faircloth
Craig Edwards
Michael Gregg
Ron Bandes
Paul Piccard

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	893BYYY789
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Printed in Canada.
1 2 3 4 5 6 7 8 9 0
ISBN: 1-59749-056-3

Publisher: Andrew Williams
Cover Designer: Michael Kavish
Page Layout and Art: Patricia Lupien
Indexer: Richard Carlson

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.

Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly are incredible, and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Kathryn Barrett, John Chodacki, Rob Bullington, Aileen Berg, and Wendy Patterson.

The incredibly hardworking team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Chris Hossack, Krista Leppiko, Marcel Koppes, Judy Chappell, Radek Janousek, and Chris Reinders for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, Joseph Chan, and Siti Zuraidah Ahmad of STP Distributors for the enthusiasm with which they receive our books.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, Mark Langley, and Anyo Geddes of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji, Tonga, Solomon Islands, and the Cook Islands.

Contributing Authors

David Maynor is a Senior Researcher with SecureWorks where his duties include vulnerability development, developing and evaluating new evasion techniques, and development of protection for customers. His previous roles include reverse engineering and researching new evasion techniques with the ISS Xforce R&D team, application development at the Georgia Institute of Technology, as well as security consulting, penetration testing and contracting with a wide range of organizations.

Lance James has been heavily involved with the information security community for the past 10 years. With over a decade of experience with programming, network security, reverse engineering, cryptography design & cryptanalysis, attacking protocols and a detailed expertise in information security, Lance provides consultation to numerous businesses ranging from small start-ups, governments, both national and international, as well as Fortune 500's and America's top financial institutions. He has spent the last three years devising techniques to prevent, track, and detect phishing and online fraud. He is a lead scientist with Dachb0den Laboratories, a well-known Southern California "hacker" think-tank, creator of InvisibleNet, a prominent member of the local 2600 chapter, and the Chief Scientist with Secure Science Corporation, a security software company that is busy tracking over 53 phishing groups. As a regular speaker at numerous security conferences and being a consistent source of information by various news organizations, Lance James is recognized as a major asset in the information security community.

Brad "RenderMan" Haines is one of the more visible and vocal members of the wardriving community, appearing in various media outlets and speaking at conferences several times a year. Render is usually near by on any wardriving and wireless security news, often causing it himself. His skills have been learned in the trenches working for various IT companies as well as his involvement through the years with the hacking community, sometimes to the attention of carious Canadian and American intelligence agencies. A firm believer in the hacker ethos and promoting responsible hacking and sharing of ideas, he wrote the 'Stumbler ethic' for beginning wardrivers and greatly enjoys speaking at corporate conferences to dissuade the negative image of hackers and wardrivers. His work frequently borders on the absurd as his approach is usually one of ignoring conventional logic and just doing it. He can be found in Edmonton, Alberta, Canada, probably taking something apart.

Thomas Porter, Ph.D. (CISSP, IAM, CCNP, CCDA, CCNA, ACE, CCSA, CCSE, and MCSE) is the Lead Security Architect in Avaya's Consulting & Systems Integration Practice. He also serves as Director of Network Security for the FIFA World Cup 2006.

Porter has spent over 10 years in the networking and security industry as a consultant, speaker, and developer of security tools. Porter's current technical interests include VoIP security, development of embedded microcontroller and FPGA Ethernet tools, and H.323/SIP vulnerability test environments. He is a member of the IEEE and OASIS (Organization for the Advancement of Structured Information Standards). Porter recently published Foundation articles for SecurityFocus titled "H.323 Mediated Voice over IP: Protocols, Vulnerabilities, and Remediation"; and "Perils of Deep Packet Inspection."

Tom lives in Chapel Hill, North Carolina with his wife, Kinga – an Asst. Professor of Internal Medicine at the University of North Carolina - and two Chesapeake Bay Retrievers.

Brian Baskin [MCP, CTT+] is a researcher and developer for Computer Sciences Corporation, on contract to the Defense Cyber Crime Center's (DC3) Computer Investigations Training Program (DCITP). Here, he researches, develops, and instructs computer forensic courses for members of the military and law enforcement. Brian currently specializes in Linux/Solaris intrusion investigations, as well as investigations of various network applications. He has designed and implemented networks to be used in scenarios, and has also exercised penetration testing procedures.

Brian has been instructing courses for six years, including presentations at the annual DoD Cyber Crime Conference. He is an avid amateur programmer in many languages, beginning when his father purchased QuickC for him when he was 11, and has geared much of his life around the implementations of technology. He has also been an avid Linux user since 1994, and enjoys a relaxing terminal screen whenever he can. He has worked in networking environment for over 10 years from small Novell networks to large, mission-critical, Windows-based networks

Brian lives in the Baltimore, MD area with his lovely wife and son. He is also the founder, and president, of the Lightning Owners of Maryland car club. Brian is a motor sports enthusiast and spends much of his time building and racing his vehicles. He attributes a great deal of his success to his parents, who relinquished their household 80286 PC to him at a young age, and allowed him the freedom to explore technology.

Tony Bradley (CISSP-ISSAP) is the Guide for the Internet/Network Security site on About.com, a part of The New York Times Company. He has written for a variety of other Web sites and publications, including *PC World*, SearchSecurity.com, WindowsNetworking.com, *Smart Computing* magazine, and *Information Security* magazine. Currently a security architect and consultant for a Fortune 100 company, Tony has driven security policies and technologies for antivirus and incident response for Fortune

500 companies, and he has been network administrator and technical support for smaller companies.

Tony is a CISSP (Certified Information Systems Security Professional) and ISSAP (Information Systems Security Architecture Professional). He is Microsoft Certified as an MCSE (Microsoft Certified Systems Engineer) and MCSA (Microsoft Certified Systems Administrator) in Windows 2000 and an MCP (Microsoft Certified Professional) in Windows NT. Tony is recognized by Microsoft as an MVP (Most Valuable Professional) in Windows security.

On his About.com site, Tony has on average over 600,000 page views per month and 25,000 subscribers to his weekly newsletter. He created a 10-part Computer Security 101 Class that has had thousands of participants since its creation and continues to gain popularity through word of mouth. Aside from his Web site and magazine contributions, Tony is also coauthor of *Hacker's Challenge 3* (ISBN: 0072263040) and a contributing author to *Winternals: Defragmentation, Recovery, and Administration Field Guide* (ISBN: 1597490792) and *Combating Spyware in the Enterprise* (ISBN: 1597490644).

Jeremy Faircloth (Security+, CCNA, MCSE, MCP+I, A+, etc.) is an IT Manager for EchoStar Satellite L.L.C., where he and his team architect and maintain enterprisewide client/server and Web-based technologies. He also acts as a technical resource for other IT professionals, using his expertise to help others expand their knowledge. As a systems engineer with over 13 years of real-world IT experience, he has become an expert in many areas, including Web development, database administration, enterprise security, network design, and project management. Jeremy has contributed to several Syngress books, including *Microsoft Log Parser Toolkit* (Syngress, ISBN: 1932266526), *Managing and Securing a Cisco SWAN* (ISBN: 1-932266-91-7), *C# for Java Programmers* (ISBN: 1-931836-54-X), *Snort 2.0 Intrusion Detection* (ISBN: 1-931836-74-4), and *Security+ Study Guide & DVD Training System* (ISBN: 1-931836-72-8).

Paul Piccard serves as Director of Threat Research for Webroot, where he focuses on research and development, and provides early identification, warning, and response services to Webroot customers. Prior to joining Webroot, Piccard was manager of Internet Security Systems' Global Threat Operations Center. This state-of-the-art detection and analysis facility maintains a constant global view of Internet threats and is responsible for tracking and analyzing hackers, malicious Internet activity, and global Internet security threats on four continents.

His career includes management positions at VistaScape Security Systems, Lehman Brothers, and Coopers & Lybrand. Piccard was researcher and author of the quarterly Internet Risk Impact Summary (IRIS) report. He holds a Bachelor of Arts from Fordham University in New York.

Frank Thornton runs his own technology consulting firm, Blackthorn Systems, which specializes in wireless networks. His specialties include wireless network architecture, design, and implementation, as well as network troubleshooting and optimization. An interest in amateur radio helped him bridge the gap between computers and wireless networks. Having learned at a young age which end of the soldering iron was hot, he has even been known to repair hardware on occasion. In addition to his computer and wireless interests, Frank was a law enforcement officer for many years. As a detective and forensics expert he has investigated approximately one hundred homicides and thousands of other crime scenes. Combining both professional interests, he was a member of the workgroup that established ANSI Standard "ANSI/NIST-CSL 1-1993 Data Format for the Interchange of Fingerprint Information." He co-authored *WarDriving: Drive, Detect, and Defend: A Guide to Wireless Security* (Syngress Publishing, ISBN: 1-93183-60-3), as well as contributed to *IT Ethics Handbook: Right and Wrong for IT Professionals* (Syngress, ISBN: 1-931836-14-0) and *Game Console Hacking: Xbox, PlayStation, Nintendo, Atari, & Gamepark 32* (ISBN: 1-931836-31-0). He resides in Vermont with his wife.

Anand Das has seventeen plus years of experience creating and implementing business enterprise architecture for the Department of Defense (DOD) and the commercial sector. He is founder and CTO of Commerce Events, an enterprise software corporation that pioneered the creation of RFID middleware in 2001. Anand is a founding member of EPCglobal and INCITS T20 RTLS committee for global RFID and wireless standards development. He formulated the product strategy for AdaptLink™, the pioneer RFID middleware product, and led successful enterprise wide deployments including a multi-site rollout in the Air Force supply chain. Previously he was Vice President with SAIC where he led the RFID practice across several industry verticals and completed global rollouts of RFID infrastructure across America, Asia, Europe and South Africa. He served as the corporate contact for VeriSign and played a key role in shaping the EPCglobal Network for federal and commercial corporations. Earlier, he was chief architect at BEA systems responsible for conceptualizing and building the Weblogic Integration suite of products. He has been a significant contributor to ebXML and RosettaNet standard committees and was the driving force behind the early adoption of service-oriented architecture. Anand has held senior management positions at Vitria, Tibco, Adept, Autodesk and Intergraph.

Anand has Bachelor of Technology (Honors) from IIT Kharagpur and Master of Science from Columbia University with specialization in computer integrated manufacturing. He served as the past chairman of NVTC's ebusiness committee and is a charter member of TIE Washington, DC. Anand and his wife, Annapurna, and their two children live in Mclean, VA.

Michael Gregg is the President of Superior Solutions, Inc. and has more than 20 years' experience in the IT field. He holds two associate's degrees, a bachelor's degree, and a master's degree and is certified as CISSP, MCSE, MCT, CTT+, A+, N+, Security+, CNA, CCNA, CIW Security Analyst, CCE, CEH, CHFI, CEI, DCNP, ES Dragon IDS, ES Advanced Dragon IDS, and TICSA.

Michael's primary duties are to serve as project lead for security assessments helping businesses and state agencies secure their IT resources and assets. Michael has authored four books, including: *Inside Network Security Assessment*, *CISSP Prep Questions*, *CISSP Exam Cram2*, and *Certified Ethical Hacker Exam Prep2*. He has developed four high-level security classes, including Global Knowledge's Advanced Security Boot Camp, Intense School's Professional Hacking Lab Guide, ASPE's Network Security Essentials, and Assessing Network Vulnerabilities. He has created over 50 articles featured in magazines and Web sites, including *Certification Magazine*, GoCertify, *The El Paso Times*, and SearchSecurity.

Michael is also a faculty member of Villanova University and creator of Villanova's college-level security classes, including Essentials of IS Security, Mastering IS Security, and Advanced Security Management. He also serves as a site expert for four TechTarget sites, including SearchNetworking, SearchSecurity, SearchMobileNetworking, and SearchSmallBiz. He is a member of the TechTarget Editorial Board.

Hersh Bhargava is the founder and CTO of RafCore Systems, a company that provides RFID Application Development and Analytics platform. He is the visionary behind RafCore's mission of making enterprises respond in real–time using automatic data collection techniques that RFID provides. Prior to RafCore Systems, he founded AlbumNet Technologies specializing in online photo sharing and printing. With 15 years of experience in building enterprise strength application, he has worked in senior technical positions for Fortune 500 companies. He earned a Bachelor of Technology in Computer Science and Engineering from IIT - BHU.

Craig Edwards is the administrator for the ChatSpike IRC network and creator of the IRC security software IRC Defender (www.ircdefender.org). IRC Defender is a security service that

keeps malicious users and programs out of IRC networks and is actively maintained to deal with current threats. Craig is also the creator of the WinBot IRC bot (www.winbot.co.uk), an automated IRC client which is designed to keep control of IRC channels, and has been instrumental in its design, maintenance, and support and web site for over five years. During this time it has been published on magazine cover CDs in the United Kingdom.

Ronald T. Bandes (CISSP, CCNA, MCSE, Security+) is an independent security consultant. Before becoming an independent consultant, he performed security duties for Fortune 100 companies such as JP Morgan, Dun and Bradstreet, and EDS. Ron holds a B.A. in Computer Science.

Contents

Foreword

Technology is a strange thing. On the grand scale of time, it wasn't so long ago that people knew everything about things they interacted with in their daily lives. If you wanted to cook something, you started a fire. If you wanted to pound something, you used a hammer or a rock. If you wanted something to grow, you watered it. It wasn't long after technology began to creep into the average person's daily life that they knew how to use it to accomplish their objectives, but not much more. A car is a perfect example of this: Most people can drive, but ask someone to change their own oil or adjust their timing belt and they are lost. Something very dangerous happened as a divide began to grow from the people who knew the intricacies of the technology and those who didn't. Unscrupulous people recognized this knowledge gap and began to exploit it. How many times have you gone to a mechanic and wondered just what a hydroflanger is and why you have to replace it so often? Of course, if you were to go to one of your friends who is knowledgeable about cars and tell them you just paid $400 to have your hydroflanger replaced, you would be greeted with a look of equal parts amusement, shock, horror, surprise and bewilderment. This is often the look I give to people when they tell me about winning the Nigerian lottery, or that they have installed a security update that got mailed to them, or they won a free iPod by punching a monkey on the Internet. Often it's just a look because I really am speechless and do not know what to say.

The IT industry and computers in general have developed this divide problem between the informed and the uninformed. Most people's interaction with their computer is checking e-mail, Web surfing, video gaming and other such tasks. Most modern computer users know how to carry out whatever task

they want, but once something goes wrong, their tech savvy friends, family or the kid down the street gets the call to help lead them out of the technical quagmire they have wandered into. The problem is not confined to just computers anymore, and it now includes: mobile phones, PDAs, and Voice over IP (VoIP. Just like in the case of the mechanic (not that all mechanics are waiting to take advantage of you), a person can be taken advantage of, suffer finical losses and a host of other bad things due to the lack of familiarity with how these new technologies actually work. Because technology is so pervasive, the average consumer can never be expected to fully understand how it all works or how to thwart hackers, but they must all be educated about how they are at risk and what they can do to protect themselves without in-depth technical expertise.

This book covers examples of the growing digital divide from many of Syngress's best authors and books. It does this from the position that there really are bad people that are out to get you and they will try to take advantage of your lack of in-depth knowledge of technology. Examples of this can include VoIP phishing, malware and spyware spreading through mediums like IM, and even the often overlooked close proximity types of attacks like wifi/Bluetooth and RFID.

I am not trying to scare you into staying away from technology altogether; I am just saying your best defense these days is developing a healthy suspicion of everything. An unsolicited e-mail probably isn't a good thing. A strange Bluetooth request in an airport probably isn't legitimate. If someone who represents themselves as customer service from your bank on the phone, you should probably hang up and call them back using the established phone numbers of your bank. Little things like this can help but the only way to truly be safe is to close the gap between the informed and the uninformed.

I wish you a very safe and happy future.

—David Maynor
Senior Researcher, SecureWorks
Atlanta GA, 2006

Part I
VoIP