[IN]SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 27 - September 2010

SANS London

November 27–December 6 2010

THE MOST TRUSTED NAME IN INFORMATION AND SOFTWARE SECURITY

- 14 OF THE WORLD'S BEST INFOSEC COURSES INCLUDING 5 NEW COURSES
- EXPERT TALKS
- VENDOR EVENTS
- COMMUNITY NIGHTS
- NETWORKING OPPORTUNITIES
- ... AND MORE!

The SANS London Experience

Be Part of It!

GIAC Approved Training

venue: ExCel London Exhibition & Conference Center
details: http://www.sans.org/london-2010/
contact: emea@sans.org

TABLE OF CONTENTS

As lowering temperatures signal the last days of summer, many of you are already behind your workstations tackling new threats and looking fondly back at the days at the beach. You're not alone, the security landscape is evidently waking up, as both black hats and white hats are back at their keyboards.

During the past few months we've been sorting through a significant number of article submissions. The result is another issue of (IN)SECURE we think you'll enjoy.

While wrapping up on this issue, we finalized our travel plans to attend ENISA's Summer School on Network and Information Security in Greece, SOURCE Conference in Barcelona and BruCON in Brussels. This means we'll be seeing many of you during September and listening to a myriad of inspiring talks. It's going to be an stimulating month!

Mirko Zorz
Editor in Chief

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Editor in Chief - editor@insecuremag.com
News: Zeljka Zorz, News Editor - news.editor@insecuremag.com
Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Distribution

The dramatic increase of vulnerability disclosures

Vulnerability disclosures are increasing dramatically, having reached record levels for the first half of 2010, according to IBM. Overall, 4,396 new vulnerabilities were documented by the X-Force team in the first half of 2010, a 36% increase over the same time period last year. 55% of all these disclosed vulnerabilities had no vendor-supplied patch at the end of the period. (www.ibm.com)

Novell releases Cloud Security Service

Novell announced the general availability of their Cloud Security Service, hosted in the cloud, either where the provider hosts its application or via a Novell hosting partner. A user can log on directly or via the enterprise identity system. The service first verifies the identity and, if successful, will generate an identity token in the format needed by the SaaS provider. (www.novell.com)

Microsoft releases mitigating tool for latest 0-day bug

HD Moore, creator of Metasploit, revealed that some 40 Windows applications are affected by a critical vulnerability that can allow attackers to execute malicious code remotely and infect the computers with malware. Microsoft released a tool that mitigates the risk by altering the library loading behavior system-wide or for specific applications. (www.microsoft.com)

New software for smarter security and compliance management

IBM announced new software to deliver security and compliance to thousands of computers globally, automating some of the most time-intensive IT tasks. The new software, delivered through IBM's BigFix acquisition, provides built-in intelligence that identifies all of a company's PCs, laptops, servers, point-of-sale and virtualized devices, then flags when devices are not in compliance. (www.bigfix.com)

The first cloud computing solution to achieve PCI compliance

Verizon Computing as a Service, or CaaS, the company's cloud computing solution is the first cloud-based solution to successfully complete the Payment Card Industry Data Security Standard (PCI DSS) audit for storing, processing and transmitting credit card information. (www.verizonbusiness.com)

DEFCON survey reveals vast scale of cloud hacking

An in-depth survey carried out amongst 100 of those attending this year's DEFCON conference in Las Vegas recently has revealed that an overwhelming 96 percent of the respondents said they believed the cloud would open up more hacking opportunities for them. (www.fortify.com)

Intel to acquire McAfee

Intel Corporation has entered into a definitive agreement to acquire McAfee for approximately $7.68 billion. Both boards of directors have unanimously approved the deal, which is expected to close after McAfee shareholder approval, regulatory clearances and other customary conditions specified in the agreement. (www.intel.com)

Resourceful attackers continue to make the web insecure

Attackers are staying one step ahead of the game and enterprises are struggling to keep up, according to a report by Zscaler. During the second quarter of 2010, attackers once again took advantage of opportunities just as quickly as they emerged. These opportunities included both the emergence of new vulnerabilities in popular technologies as well as current events that drew the attention of millions around the globe. (www.zscaler.com)

Secure remote access for Mac users

HOB launched MacGate, a new secure remote access solution designed specifically for Mac users. It provides users with access to computers running Mac, especially graphics workstations, on a corporate network either through a LAN or over the Internet. (www.hobsoft.com)

Employees admit they would steal data when leaving a job

Employees openly admit they would take company data, including customer data and product plans, when leaving a job, according to Harris Interactive. The online survey probed 1,594 full- and part-time employees and contractors in the United States and Great Britain about their attitudes toward accessing and viewing of company-owned data. (www.harrisinteractive.com)

Publicly trusted secure e-mail certificates

Entrust adds publicly trusted secure e-mail certificates to its certificate management service, enabling digital signature capabilities and encryption of e-mails and other documents. Based on the X.509 certificate standard, Entrust Secure E-mail Certificates enable standards-based S/MIME capabilities. (www.entrust.com)

PCI standard changes ahead

The PCI Security Standards Council published documentation highlighting the expected changes to be introduced with version 2.0 of the PCI DSS and PA-DSS in October 2010. Version 2.0 of PCI DSS and version 2.0 of PA-DSS do not introduce any new major requirements. (www.pcisecuritystandards.org)

Millions of Coldfusion sites need to apply patches

ProCheckUp were able to access every file including username and passwords from a server running ColdFusion. This was completed through a directory traversal and file retrieval flaw found within ColdFusion administrator. A standard web browser was used to carry out the attack, knowledge of the admin password is not needed. (www.procheckup.com)

D-Link routers get DNSSEC and CAPTCHA protection

D-Link enhanced its router security by incorporating both CAPTCHA and DNSSEC to guard against hacking, worms, viruses and other malicious Web attacks. (www.dlink.com)

Loss of personal information as stressful as losing a job

Americans feel most vulnerable about the loss or theft of their personal or financial information. Fifty-four percent of Americans said the prospect of losing this data “extremely concerned” them (based on a rating of eight or higher on a 10-point scale). Losing personal or financial information ranked similar to concern over job loss (53 percent) and not being able to provide healthcare for their family (51 percent). (www.antiphishing.org)

Security check for broadband home routers

Attackers are increasingly targeting home routers as a means of gaining access to sensitive personal data. To help combat this threat, ICSA Labs is offering a new program under which manufacturers can have broadband home routers certified. The program, Broadband Home Router Certification, evaluates a router's effectiveness in identifying safe versus harmful data, and denying access to malicious data. (www.icsalabs.com)

64GB secure portable USB drive

MXI Security offers a 64GB device for its Stealth line of secure USB devices, suited for customers that require devices for the secure portable desktop that allows you to natively boot Microsoft Windows from a Stealth USB device. (www.mxisecurity.com)

Wipe technology for self-encrypting disk drives

Toshiba announced Wipe for Toshiba Self-Encrypting Drive models, a technology that allows special security capabilities, such as the world's first ability for sensitive user data to be securely erased when a system is powered-down or when a SED HDD is removed from the system. (www.toshiba.com)

Free protection against Blackhat SEO threats

Zscaler released Search Engine Security, a free solution specifically designed to combat Blackhat SEO attacks. With a typical anti-virus detection rate below 25% for such attacks, the protection provided by this solution can be a valuable asset in keeping PCs from falling victim to Blackhat SEO attacks. (www.zscaler.com)

Former SF network admin Terry Childs sentenced to prison

After a drawn out trial that saw City of San Francisco administrator Terry Childs being convicted of violating California state hacking laws by deliberately locking the authorities out of the city's FiberWAN network by refusing to disclose administrative passwords, he has finally been sentenced to four years in prison.

Private browsing modes not as private as one might wish

The four most used web browsers - Internet Explorer, Firefox, Chrome and Safari - all have private browsing modes. Yes, they are designed to delete the most obvious signs of online activity such as cookies, browsing history and the browser's cache, but is that enough to keep your surfing habits hidden from interested parties?

Review: BlockMaster SafeStick SuperSonic

by Mark Woodstone

Swedish company BlockMaster is a new player on the secure USB flash drives market. Their flagship products include SafeStick USB drive and SafeConsole platform for centralized USB management. I have been using their 8 GB SafeStick drive for half a year now and I like the combination of the product's performance and its capability of working on multiple platforms.

I use SafeStick SuperSonic, an upgraded version of the baseline secure USB product. This ultra fast device comes in sizes of 4 and 8 Gigabytes, while the regular ones can reach a size of up to 128GB.

Although the company web site labels the device as "the world's fastest USB flash drive", I think they forgot to add the word "secure" into the statement. The benchmarks that inspired the catchy title compared SuperSonic with other encrypted USB drives, not with USB flash drives in general.

According to the benchmark tests from independent labs (unfortunately not specified), the tested SafeStick SuperSonic 4GB has the overall best results when compared to the "plain" SafeStick and three other unnamed competitors.

Methodologies used include classic copying of file to the device, using ATTO Disk Benchmark and Harald Bögeholz's H2testw. The benchmark report can be downloaded on the following web page: http://tinyurl.com/3xdfkro. Although I didn't do any speed tests, from my active usage I can say that performance is good and it seems to be working faster than similar devices I have used in the past.

SafeStick SuperSonic has a slick slim chassis and it seems to be quite rugged.

BlockMaster did a number of tests on it including whacking it with a sledgehammer, rolling over it with a V8 Range Rover, and even washing it repeatedly in the washing machine under high temperatures.

When I read this, I was tempted to try out some destructive ideas of my own, but common sense prevailed.

As a side note: you can look for these "attacks" on SafeStick's integrity on YouTube.

From the security point of view, SafeStick SuperSonic sports an always-on automatic hardware AES256 encryption in CBC mode. The encryption keys are generated on board the device in the user setup procedure. After you authenticate, the device acts just like your typical USB flash drive.

I mentioned earlier that it works on multiple platforms. When you plug the drive into your Windows machine it automatically provides you with a login application - you enter your password and it's ready for you to use. Mac OS X users need to download a small (1.6 MB) software package that provides the same functionality.

SafeStick SuperSonic is ready for the enterprise through the SafeConsole centralized USB management platform, which has the power to serve 100,000+ SafeStick deployments.

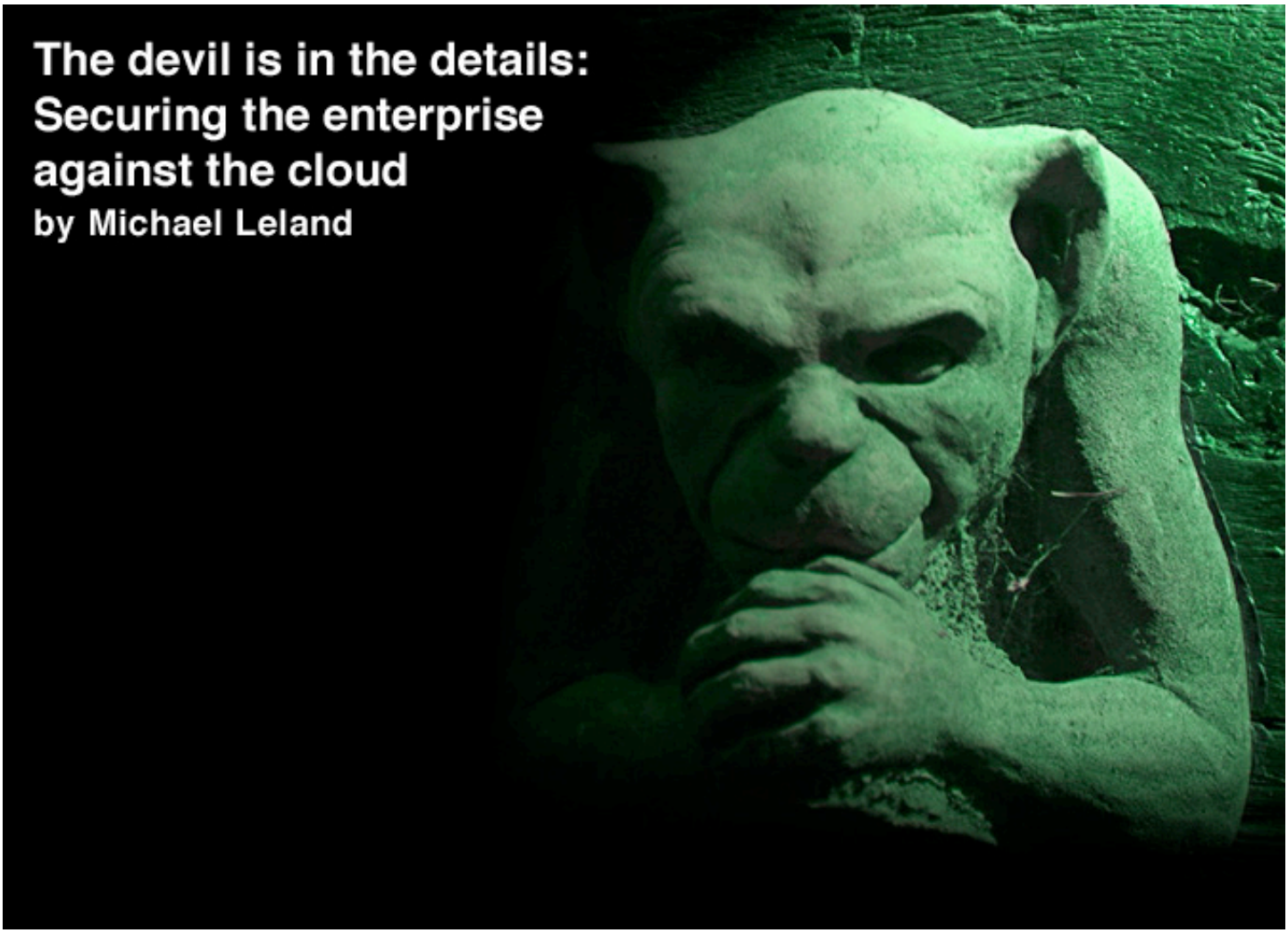
Cons: slight overheating when connected to some external USB hubs.

Pros: performance, slim design, works on both Windows and Mac OS X, enterprise ready.

Mark Woodstone is a security consultant that works for a large Internet Presence Provider (IPP) that serves about 4000 clients from 30 countries worldwide.

The devil is in the details: Securing the enterprise against the cloud

by Michael Leland



Network visibility continues to be a necessary and important part of information security, but in this era of social networks and Web 2.0 it is no longer entirely sufficient. The main problem is that content continues to move away from corporate servers, into the less visible and manageable cloud. Because of this shift, the ways in which we monitor and secure our business applications must also change.

The cloud remains difficult to secure for many reasons: the computing platform is highly distributed; the platforms are often virtual; but perhaps the most challenging quality is its diversity. Cloud services can theoretically be accessed by anyone, from anywhere, putting the security onus almost exclusively on user authentication.

Whether or not the cloud can ever be truly secured is a matter of debate: even if it's possible to control access to cloud services, enforcing behavior in the cloud can be extremely difficult.

Discussions about cloud security often focus on strong authentication and trying to protect the cloud service itself, but let's forget for a moment the issue of securing the cloud and think about what else connects to it.

Does the cloud connect back to anything within your enterprise network? It is becoming commonplace for companies to use a web-based CRM - it's an excellent service and provides lots of value. However, those companies also host their own corporate web servers, and have tightly integrated their intranets with their customer-facing CRM, in order to deliver valuable internal tools for business intelligence.

The integration is done the correct way, using published APIs. The web servers themselves are protected behind firewalls and intrusion prevention systems, so the assumption is that

everything is safe. But is their cloud-based CRM fully secured? And more importantly, if it were to be compromised, could it be used to access my web server using the legitimate account credentials and security tokens of the API?

The short answer is: yes, it could.

This is just one example, of course. There are numerous ways to tie cloud based services back into our enterprise data centers, and the simplest advice for avoiding the introduction of open backdoors to our otherwise secured networks is to avoid implementing those connections in the first place.

However, as companies grow more dependent upon web-based services in order to make their own distributed workforce more efficient, that advice becomes hard to follow. Let's face it: being able to access and track a customer's order via their intranet login is a good thing, and being able to gauge productivity of your manufacturing or assess the market acceptance of a product line from a web-based dashboard can be extremely helpful. That means tying the two (or more) systems together, and that means introducing new risks.

So what can we do? If we could see how our internal systems were interacting with other users, services, and applications on the network, we could proactively watch these backdoors. We could make sure that inbound connections from the cloud were being used appropriately, by legitimate accounts, and for legitimate reasons.

The bad news is that this level of monitoring requires full application session decoding, in order to analyze the actual contents of those connections at the application layer. The good news is that this advanced technology exists today.

THERE ARE NUMEROUS WAYS TO TIE CLOUD BASED SERVICES BACK INTO OUR ENTERPRISE DATA CENTERS, AND THE SIMPLEST ADVICE FOR AVOIDING THE INTRODUCTION OF OPEN BACKDOORS TO OUR OTHERWISE SECURED NETWORKS IS TO AVOID IMPLEMENTING THOSE CONNECTIONS IN THE FIRST PLACE.

Understand the connection

Unlike typical networks, which are dependent upon the physical, datalink and network layers to establish a connection, cloud services are more likely to be delivered (and authenticated) over a web browser or some other application. They're abstracted away from the network, and operate more at the session and application layer.

This means that you not only need to look at connectivity as something that occurs "further up the stack," but you also need to fully understand how that connectivity should behave, as well as how it is behaving.

Authentication should be strict and hard, and as much additional context as possible should be applied to it. That authentication should also never be trusted, because when an attack comes in from the cloud, there's a good chance that it will be using trusted accounts and certificates.

This is where an analytical tool such as a SIEM (Security Information and Event Manager) comes into play, because you need to collect user access information from the service itself, correlate that to your own user authentication system, establish baseline behaviors and policies, and set up alerting to inform you when something suspicious is going on. In other words, you need to correlate events and behavior from both the cloud and your enterprise network.

To gain real insight, that correlation will incorporate the monitored behavior of the connection between the two environments. That's an enormous amount of data correlation, and requires automation to make it operational.

Monitor the connection

Understanding the nature of how cloud services authenticate and connect enables you to monitor those connections appropriately. A new type of monitoring is required to enable security analysts to look inside the contents of applications in order to enforce data access and usage policies that are being mandated by SOX, PCI, HIPAA and other compliance regulations.

We're already looking at the cloud server logs (which should be collected locally by your enterprise SIEM), your own identity and access management (IAM) system, and – to the best of your abilities – network connections between the outside world and the cloud. The next step is to implement layer 7 application monitoring, to look inside those connections to ensure that the connection is legitimate and not spoofed; that the user is not transferring sensitive information to or from the cloud; and look for any number of other suspicious activities that occur within a session once it has been established.

Again, you'll want some heavy-lifting analytic tools in your corner to help automate this, and to correlate everything together. You'll also need a layer 7 monitoring device that can actually decode and inspect the contents of applications.

The details

While these tools are available today – in the form of application data monitors, content firewalls, DLP, other data-inspection products, and SIEMs – products alone can't secure the cloud. Application monitoring gives you visibility up through layer 7, but that visibility doesn't do you any good if you don't know what you're looking for.

Are the underlying protocols legitimate? Have sessions been established correctly? Once a session is established, what is the user doing, and does that behavior indicate any type of risk?

Take the time to tune your monitoring and alerting tools according to your own usage policies, and you'll be able to monitor application use within the context of your own internal usage policies, not to mention whatever compliance requirements you are held to.

The devil

If you manage to control and monitor all access to your cloud service, you'll be faced with an additional challenge: encryption. When re-directing and monitoring outside access, you'll need to decrypt that session before it can be monitored.

Internally, you have your own certificates and can simply terminate the secure connection prior to monitoring. When things aren't in your control – and they rarely are when dealing with virtualized, distributing computing – it means that you need to find another way to unlock those sessions.

Is it appropriate to recommend implementing a man-in-the-middle within your own network? Using an SSL decoding appliance industrializes the process somewhat, making it seem more legitimate, but the truth is that you have to act a bit like the devil in order to get the details.

The good news is that there's hope. With a little effort to control how cloud services are accessed, and by correctly monitoring that access, it's possible to regain a clear picture of how your applications and information are being used, in order to truly defend against data loss and theft.

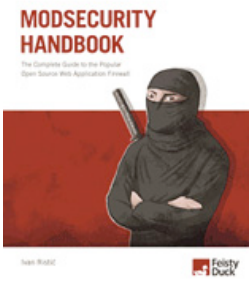
- Collect logs from your cloud server(s), especially those involving user access and activity
- Establish a whitelist of authorized users and privileges from your own authentication system
- Monitor traffic aggressively so that you have as much data as possible about cloud activity
- Centralize everything, correlating network-, user- and application-level activity together.

Michael Leland serves the office of the CTO at NitroSecurity (www.nitrosecurity.com). He is responsible for developing and implementing the company's overall technology vision and roadmap including next-generation network and security management solutions.

ModSecurity Handbook

By Ivan Ristic

Feisty Duck, ISBN: 1907117024

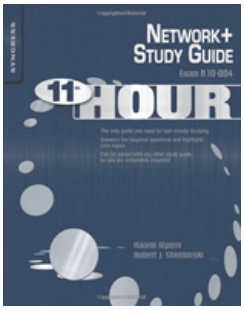


ModSecurity Handbook is the definitive guide to ModSecurity, a popular open source web application firewall. Written by Ivan Ristic, who designed and wrote much of ModSecurity, this book will teach you everything you need to know to monitor the activity on your web sites and protect them from attack. The book is suitable for all reader levels: it contains step-by-step installation and configuration instructions for those just starting out, as well as detailed explanations of the internals and discussion of advanced techniques for seasoned users. Includes the official ModSecurity Reference Manual.

Eleventh Hour Network+: Exam N10-004 Study Guide

By Naomi Alpern

Syngress, ISBN: 1597494283



The 11th Hour Network+ Study Guide is keyed to the N10-004 revision of the CompTIA Network+ exam. This book is streamlined to include only core certification information and is presented for ease of last-minute studying. Main objectives of the exam are covered with key concepts highlighted: Fast Facts quickly review fundamentals, Exam Warnings highlight particularly tough sections of the exam, Crunch Time sidebars point out key concepts to remember, Did You Know? sidebars cover sometimes forgotten details, Top Five Toughest Questions and answers help you to prepare.

Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance (2nd Edition)

By Jazib Frahim and Omar Santos

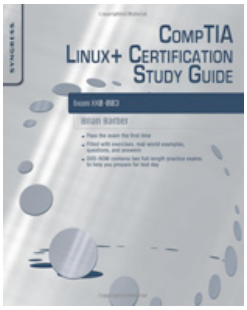
Cisco Press, ISBN: 1587058197

This book is Cisco's authoritative practitioner's guide to planning, deploying, managing, and troubleshooting security with Cisco ASA. Readers will learn about the Cisco ASA Firewall solution and capabilities; secure configuration and troubleshooting of site-to-site and remote access VPNs; Intrusion Prevention System features built into Cisco ASA's Advanced Inspection and Prevention Security Services Module (AIP-SSM); and Anti-X features in the ASA Content Security and Control Security Services Module (CSC-SSM). This new edition has been updated with detailed information on the latest ASA models and features.

CompTIA Linux+ Certification Study Guide (2009 Exam): Exam XK0-003

By Brian Barber, Chris Happel, Terrence V. Lillard, Graham Speake

Syngress, ISBN: 1597494828

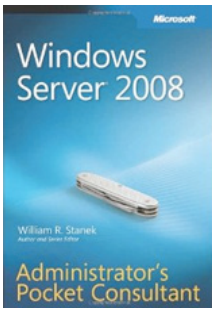


CompTIA's Linux+ certification is a globally-recognized, vendor neutral exam. The Linux+ exam (XK1-003) is a substantive revision with updates on applications, networking, and security. This new study guide is aligned to cover all of the material of the updated 2009 exam with special attention to the new topics including troubleshooting Web-related services, understanding DNS record types and resolving them, and the basics of SELinux security.
The study guide will cover installing applications, configuring the base system, using BASH, and securing and maintaining Linux.

Windows Server 2008 Administrator's Pocket Consultant

By William R. Stanek

Microsoft Press, ISBN: 0735624372

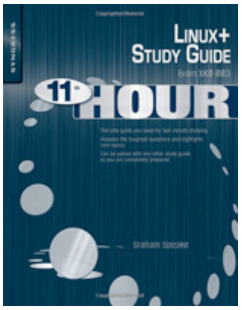


Designed for quick referencing, this portable guide covers all the essentials for performing everyday system administration tasks. You'll discover how to manage workstations and servers, use Microsoft Active Directory directory service, create and administer user and group accounts, manage files and directories, back up and recover data, and use TCP/IP, WINS, and DNS for network administration. Featuring quick-reference tables, concise lists, and step-by-step instructions, this handy, one-stop guide provides fast, accurate answers on the spot whether you're at your desk or in the field.

Eleventh Hour Linux+: Exam XK0-003 Study Guide

By Graham Speake, Brian Barber, Chris Happel and Terrence V. Lillard

Syngress, ISBN: 1597494976



The 11th Hour Linux+ Study Guide is keyed to the XK0-003 revision of the CompTIA Linux+exam. This book is streamlined to include only core certification information and is presented for ease of last-minute studying. Main objectives of the exam are covered with key concepts highlighted: Fast Facts quickly review fundamentals, Exam Warnings highlight particularly tough sections of the exam, Crunch Time sidebars point out key concepts to remember, Did You Know? sidebars cover sometimes forgotten details, Top Five Toughest Questions and answers help you to prepare.

RSA CONFERENCE
EUROPE 2010
12-14 OCTOBER | HILTON LONDON METROPOLE | U.K.

SECURITY DECODED

Stay ahead of information security threats. Attend RSA® Conference Europe 2010.

Deciphering our changing security landscape gets more daunting by the day. RSA® Conference Europe 2010 has the solutions. Over three days, get the practical knowledge you need to protect and secure your organisation. Benefit from:

- 70 educational track sessions
- Keynotes from industry thought leaders and guest speakers
- Interactive programmes
- Demonstrations from leading vendors
- Time to meet and collaborate with peers

Dates: 12th – 14th October
Venue: Hilton London Metropole Hotel, UK

Register Early and Save!

Discount Registration
17th July – 10th September:
£850 + VAT

Standard Registration
11th September – Event:
£975 + VAT

Register online now at:

www.rsaconference.com/2010/hn

Cybercrime may be on the rise, but authentication evolves to defeat it

by Steve Dispensa

Cybercrime is a fact of modern life, and its continued rise in prominence has caused the media, various politicians, and even the general population to start to take notice. It's all but certain that the next major war will include a cyberwarfare component, and the U.S. government is rushing to do what it can to build competency in computer-related defense.

We've already begun to see the first echoes of this sort of activity, in cases like the Aurora exploit that targeted Google and others in early 2010. Closer to home, cybercrime is starting to make a significant impact on the bottom lines of businesses, especially in the financial sector, but often elsewhere as well.

Part of what has been driving the continued increase in cybercrime rates has been the relatively rapid adoption of technology by organized crime rings over the past five years. Cybercrime is no longer the provenance of teenagers in their parents' basements – it is now a business with a legitimate model, funded by wealthy and motivated organizations, with access to some of the world's top computing talent.

Cybercrime can be roughly divided into two categories: targeted attacks and bulk attacks. Targeted cybercrime is nothing new, although like bulk cybercrime, it has increased in recent years. Targeted cybercrime involves a criminal targeting a particular individual or business, often using some specific knowledge about the situation. Recent insider attacks fall under this heading.

Even more concerning, though, is the explosion of bulk crime. Using tools such as the Zeus malware program, criminals are able to mount an attack on a huge number of targets at once, which are generally not known to the attackers in advance. Zeus is still active over three years after its initial identification, and as of July 2010, it is estimated to control over 3.6 million computers in the U.S. alone.

Bulk attacks have become so problematic that, in late 2009, the FBI, together with the American Banking Association, released guidance to all users of business online banking that recommended that they use a dedicated

computer for online banking, and for nothing else, in an effort to limit the possibility of becoming infected by one of these pieces of malware. While this advice could potentially put a dent in infection rates, it is more striking for its tacit admission of the size of the problem and the lack of a quick, effective solution.

Software vulnerability defense mechanisms have included a variety of approaches over the years, including firewalls, IDS systems, and anti-malware software. These defenses have indeed been effective at mitigating the exploitation of software vulnerabilities over time, but as these defenses improve, attackers simply pick another angle. Increasingly, that new angle is attacking user authentication.

Multi-factor authentication

As it has become more and more difficult to exploit software flaws, attackers have naturally looked for an easier target: authentication systems. These attacks go back several years, starting with early keystroke loggers that captured passwords, and moving on to email-based phishing attacks that netted attackers thousands of credentials at a time. Authentication attacks have continued to increase in sophistication over the years, and are now a basic part of many of the most serious bulk attacks being reported today.

When authentication is the problem, a natural reaction is to deploy strong authentication solutions, and such systems have indeed seen wide deployment over the past several years.

The exact definition of strong authentication varies from situation to situation, however. In some sectors, strong authentication can mean simply asking for answers to security questions (e.g., “what is your favorite color?”). In other contexts, it can involve other factors, such as biometrics, location, time of day, and more.

A subset of these strong authentication technologies are “multi-factor” technologies, which require the user to present more than one authentication factor from a specific list of possibilities, including “something you know” (passwords, pin numbers, and such), “something you have” (including phones, smart cards, security and tokens), or “something you are” (biometric authenticators, like retinal scans, voice prints, fingerprints, and so on). Multi-factor solutions are either two-factor or three-factor, and these factors must be of different kind to qualify – you can’t use two things from the “something you know” category, such as a password and a pin.

There are systems that are referred to as multi-factor authentication systems, but do not meet this definition. These systems may make use of web browser characteristics, IP geolocation, usage patterns, time of day, and so on - all of which is useful information for authenticating users, but it doesn’t enjoy the same near-universal approval of the security community that the three traditional categories do.

Out-of-band authentication

Recently, an additional distinction among the various multi-factor systems has emerged: in-band versus out-of-band. In-band systems collect both (or all three) factors via a single logical channel, and out-of-band systems use at least two different channels to collect the factors. A common example of an in-band system is token-based authentication – users transmit the something they know (their memorized PIN number), together with the something they have (evidence of possession of the token, in the form of a temporary token code), over the same channel, the Internet.

The weakness of the in-band system lies in the fact that a single piece of malware, on a single system, can attack both factors simultaneously. In the token example, all that would be required to attack the system would be a piece of malware that captures the input data (the PIN + token code) and transmits it to an attacker via some mechanism such as IM. When the attacker receives the information, he simply uses it to log in, and the server can’t tell the difference between that attack and a legitimate login from that location.

A solution to this problem is to use out-of-band authentication, where the factors are collected via different logical channels. Phone-based authentication is the most common and widely used out-of-band authentication method.

It works by collecting the something you know via the Internet and verifying the something you have (possession of the telephone) via the phone network. In this way, it's impossible for a single piece of malware to attack both factors simultaneously.

Transaction verification

Authentication of logins is critical, but in the face of the newest, most sophisticated attacks, it can be insufficient. Again, once one attack becomes too difficult to mount, criminals simply look for the next-easiest approach. When it becomes too difficult to attack the authentication step, attackers will simply bypass it with malware. These attacks aren't theoretical, either; there have been several reported cases, relating to malware like Zeus and Clampi, of post-authentication attacks.

One attack works like this: the user's computer is infected with a malware program, which patiently waits for the user to log into an online banking site. It can't bypass authentication due to the presence of strong authentication technology, but it doesn't need to – it simply waits for the user to log in. Once logged in, the malware sends commands to the bank to do things like transfer money, all without showing what it's doing to the user, who may just be trying to check a balance or enter an online bill pay request.

The bank cannot differentiate between the fraudulent transaction and a legitimate one, and unless the user is particularly vigilant at reconciling account statements, the transaction can easily be missed until after it has cleared. At that point, exactly who is responsible for the loss is unclear, but generally, liability has been incurred by the bank's customer, not by the bank itself. (Note that this is a rapidly evolving area of law; at least one lawsuit is pending challenging this arrangement.)

Even more insidious attacks are possible. Imagine a piece of malware that simply waits for online banking customers to enter ACH transactions, and then changes only the destination ABA and Account numbers. The customer's balance would still look right, and except for in the case of an incredibly vigilant (and detail-oriented) bookkeeper, this problem won't be noticed for weeks – until the intended recipient complains about the missing payment.

The root of the problem is, once again, an authentication issue. The transaction was not initiated by the authenticated user – it was initiated by an unauthenticated security principle represented by the malware. The solution, then, is to re-authenticate the user at transaction time. Authenticating the transaction itself prevents malware from slipping in an unrequested transaction.

Considering the above example, assume that the online banking application was protected by phone-based transaction verification. Upon receipt of the ACH transfer request, the bank's servers would initiate a phone call to the user who (ostensibly) made the request, and would play back the transaction details to the user and ask for confirmation. The user would, of course, deny the transaction, and the money would never leave the bank account.

Transaction verification can ask for more than a simple authentication of the user, however. Even the account number switch described above can be detected by asking the user to re-enter part of the destination account number during the confirmation call. This is an easy request to comply with, since generally the user has the destination account number in front of him or her at the time the call is made, and it's an effective prevention of an account number switch attack.

In fact, these are both special cases of transaction data signing (TDS). By requesting that the user re-authenticate, or sign, each piece of the transaction, the bank can have a high degree of confidence in the authenticity of the request. A full TDS request might include the date, source and destination account numbers, and transaction amount, together with an authentication code. Banks can generally reach the desired level of authentication security using only a subset of this information.

Transaction verification goes beyond online banking, of course, to any context in which sensitive transactions are taking place. The concept could apply to changing files on a file server, or even to accessing specific web pages for reading data.

Common web single sign-on and authentication solutions customarily separate documents by required authentication level, and at least two common systems, IBM Tivoli Access Manager and Computer Associates SiteMinder, support step-up authentication using phone-based authentication. Defining the appropriate level of access granularity in an application can be difficult. Security administrators have to balance the desire for authentication security against users' desire not to be excessively bothered by re-authentication requests during the normal course of business.

Various additional tools can be brought to bear to make the common usage scenarios convenient for the user while still maintaining an appropriate level of security, including IP-based whitelists for authentications coming from trusted corporate computers, or transaction authentication caching, including not re-authenticating successive similar transactions. For example, it may make sense not to re-authenticate an ACH transfer to a given destination account after the first authentication succeeds.

Transaction verification can be implemented in a number of ways. We have described phone authentication as one possibility; another is SMS-based authentication, where the details of the transaction are sent via SMS text message to a user's mobile phone. The user then replies to the SMS message out-of-band to confirm the transaction. In addition, there are various smart card-based solutions that do full transaction data signing, although they haven't seen wide deployment to date due to cost and logistical considerations.

These systems generally involve the use of a smart card together with a special-purpose smart card reader with a numeric keypad that can be used to enter and sign transaction details.

There are a variety of challenges involved in transaction verification. Most applications (outside of certain government situations) lack the concept of transaction or event confirmation. These applications simply don't have a mechanism for requesting authentication at arbitrary points within the workflow. Applications such as these will either require source code modifications or a proxy solution. Beyond the basic capability, setting up a system for transaction confirmation can be tricky, because of the potentially complex rule set dictating when additional authentication is necessary and the tension between ease of use and authentication security. Centralized access management systems can be of help in heterogeneous web environments, but security administrators are largely left on their own when dealing with individual line-of-business applications.

Going forward

The world has changed. Cybercriminals are making an excellent living attacking authentication systems, and security administrators have the difficult task of defending the users against these attacks. So, where do we go from here? Companies should include a comprehensive authentication security analysis in the planning stage of every significant new application that the organization deploys. Try to focus on applications that have support for granular, event-based authentication, or consider proxy-based solutions. Look to out-of-band authentication methods to protect against in-line threats.

Finally, start analyzing existing applications for potential weaknesses in the authentication architecture. Transactions that are particularly high-risk should be protected by transaction verification; press vendors for transaction verification support or add it yourself.

Steve Dispensa is CTO & co-Founder of PhoneFactor (www.phonefactor.com). His many accomplishments include designing one of the world's first broadband wireless Internet networks for Sprint, as well as being a five time winner of the Microsoft Most Valuable Professional award. Steve, along with PhoneFactor developer Marsh Ray, recently discovered the TLS/SSL Authentication Gap – a major vulnerability in SSL authentication making it vulnerable to man-in-the-middle attacks.

Here are some of the Twitter feeds we follow closely and can recommend to anyone interested in learning more about security, as well as engaging in interesting conversations on the subject.

If you want to suggest an account to be added to this list, send a message to **@helpnetsecurity** on Twitter. Our favorites for this issue are:

@hal_pomeranz

Hal Pomeranz - Independent IT security consultant, SANS Institute faculty fellow.
http://twitter.com/hal_pomeranz

@wimremes

Wim Remes - Information security manager at Ernst & Young.
http://twitter.com/wimremes

@RafalLos

RafalLos - Security evangelist, blogger, and WebAppSec SME at HP.
http://twitter.com/RafalLos

@CiscoSecurity

Security technology, events and news.
http://twitter.com/CiscoSecurity

We security folks are often blamed for treating our users (or customers, if you want) as less than competent. We generally expect users to consider what we say as information security gospel, but that doesn't happen very often.

Many users have questions, and if we are lucky they may voice them. Personally, I have found that when I take the trouble to explain the reason behind my decree, people are more likely to comply. You can file that under the "user education" category, if you will.

I have a small home server that I use and abuse for various purposes, and tracking the various trends and attempts of ssh bruteforcing has always been a source of endless amusement. But one day, the following questions sprung into my mind: "Could I actually use that information? Could I get something useful from it?"

With that in mind, I set about working on starting logging the passwords. I will not go into the details now - suffice to say I wanted something that was low maintenance, worked and did not require another server process or modifying the sshd code.

I ended up using a custom pam module to log the source, the username and the password of each attempt, and I created honeypot users to monitor these attempts.

Each bruteforce attempt creates a log entry that looks something like this:

```
host = estpak.ee : username = shoutcast : password = shoutcast
```

I let that setup run for a few months, specifically from December 2009 to July 2010. Let's see if the collected data can help us answer some questions.

Question 1: No-one wants to attack us, do they?

Most of us don't like to think that people are actively out to get us. But, let's look at the statistics regarding the 8-month period in question:

• Total Attempts: 159969
• Unique Sources: 728
• Monthly Average: 19996
• Daily Average: 658
• Unique Usernames: 16155
• Unique Passwords: 16445.

According to this, a large number of people are engaged in attacking (and yes, I realize that some of the attacks are coming from compromised machines and that their owners might not be aware of them being used to do this, but regardless of intent, the attacks are still happening). In fact, every day attacks from roughly 3 new sources were detected. Add this information to the number of total attempts, and you can see that everyone on the Internet is a target for someone else.

Question 2: Why do I have to select a good password?

What makes a good password is a topic on which a lot can be said, but I do not want to address it in this article. I simply wanted to show which passwords bruteforcers attempt to use most commonly. Here is a top 10 list:

PASSWORD	NUMBER OF ATTEMPTS
123456	2103
password	1267
test	869
1234	814
root	753
oracle	736
qwerty	707
12345	622
abc123	615
redhat	600

This list is perfect for learning which passwords to avoid using.

Let's see some more statistics:

• Passwords consisting of 10 or more characters: 15949 (17% of total)
• Passwords consisting of 6 or less characters: 44552 (48% of total)
• Passwords consisting of 3 or less characters: 4815 (5% of total)
• Passwords containing special characters: 7055 (7% of total)
• Passwords containing only numeric characters: 10830 (11% of total)
• Passwords containing only alpha characters: 41349 (44% of total).

Going by these numbers, the simple act of using special characters in the password negates 93% of all attacks – it's something to think about.

A figure on the following pages takes a closer look at one of the most common passwords I found, and at all the ways it was used.

This figure shows us that even though the word "password" was used 1267 times, variations of that word were used 3691 times - almost 3 times more. And if you look at some of the permutations, you will notice that special characters were used. So, even if using special characters negates 93% of the attacks, it does not mean you can afford to pick a common/popular password.

1	P455W0RD	1	P@SSW0RD	16	p455word	19	P@$$word	42	pa55word
1	p4sSw0rd	1	P@SSWORD	16	p455wOrd	20	P455w0rd	56	Password
1	p4Ssw0rd	1	P@$$W0RD	16	P455word	20	PasswOrd	61	p4ssw0rd
1	P4SSW0RD	1	P@$$WORD	16	P455wOrd	22	P4ssw0rd	86	p@ssword
1	P4SSWORD	2	p4$$w0rd	16	PaSsWoRd	24	Pa$$w0rd	102	P@ssw0rd
1	P4$$w0rd	2	P4$$W0RD	16	pa$$word	24	P@$$w0rd	337	pa55w0rd
1	p4$$word	2	PA$$WORD	17	p@55wOrd	29	P@55w0rd	457	p@ssw0rd
1	P4$$word	3	Pa$$word	17	P@55wOrd	32	p@$$w0rd	482	passw0rd
1	P4$$WORD	5	Pa55word	18	p@55word	33	P@ssword	1255	password
1	P@55W0RD	7	p4s5w0rd	18	passwOrd	34	P@55word		
1	P@55WORD	8	Pa55w0rd	18	p@sswOrd	36	PASSWORD		
1	PA55WORD	13	pa$$w0rd	18	P@sswOrd	38	p4ssword		
1	PASSword	14	p4sswOrd	18	p@$$word	39	Passw0rd		
1	p@sSw0rd	14	P4sswOrd	18	p@$$wOrd	41	p455w0rd		
1	p@Ssw0rd	15	P4ssword	18	P@$$wOrd	42	p@55w0rd		
Total: 3691									

Let's take a look at the top 20 used passwords containing special characters:

PASSWORD	NUMBER OF ATTEMPTS
p@ssw0rd	457
!@#$%^	128
Sh3l5Lik3P4rtY@v3r	111
P@ssw0rd	102
p@ssword	86
!@#$	76
!@#$%^&*	67
67 !@#$%	67
!@#$%^&*()	64
!@#	62
!@#$%^&	61
QAZwsx!@#	44
zh3l5Lik3P4rtY@v3r	42
p@55w0rd	42
!@#$%^&*(	42
QQAAZZwwssxx!!@@##	39
qaz123$	36
QAZ!@#123	34
P@55word	34
P@ssword	33

What does this list show us? We can see that not only words and word variations are used, but that a large number of keystroke sequences are used, as well.

The conclusions drawn from the collected data confirm the advice we give users about the need of choosing good passwords.

Question 3: Won't they go away after a few tries?

This question is generally asked by people who are unable to ignore the evidence that points to the fact that they are being attacked, but are also unable to believe that it is as bad as all that.

Let's see what the data tells us, shall we?

The table on the following page showcases the top 15 sources and the number of attacks they mounted (per month):

SOURCE	Dec.	Jan.	Feb.	Mar.	Apr.	May	Jun.	Jul.
59.46.39.204	528	30	892					
218.234.33.31					1120			
64.15.66.147								3348
218.15.143.94	905							
222.68.194.69	113	211	77	600	204	51	58	768
web.digitalchild.com	3892							
222.236.44.99						4522	693	
81.168.140.114				1500				
202.100.108.25				1440				
58.61.156.195			2680		378	740		
218.240.40.108				1977				
188.95.105.220							3476	
e010.enterprise.fastwebserver.de		2223						
smsbravo.com							5455	
correo.correoprofesional.net			31546					

From this we can see that a large number of attackers seem to be active only for a month or two. But 5455 attempts in a single month from sms.bravo.com are nothing to sneeze at, even if the attacker gave up trying after that.

We can also see that some attackers are rather persistent - the attacker behind 222.68.194.69 shows up every month.

Let's see which behavior is more dangerous:

SOURCE	Total unique usernames	Total unique passwords
smsbravo.com	651	2975
222.68.194.69	26	388

While smsbravo.com attacked only for a month, this activity presented more danger to us then the one in which 222.68.194.69 engaged, since it comprised of a larger number of unique attempts. This collected data shows that many attackers "go away" after a certain period but, more importantly, that these attackers can be just as dangerous as - and often more than - those attackers who persist for months.

Conclusion

I understand that this dataset is a fairly 'narrow' collection, since it is focused on ssh bruteforcers, and was not taken from multiple servers in a large corporate address space. I know that there are many pieces of advice for preventing just these types of attacks, and yes, I purposely ignored all of them. And I know that answering these types of questions may seem like a waste of time to most of us, and I can imagine security people saying: "Of course the data will confirm what we say".

Nonetheless, I believe this type of analysis is useful to show people why we say and recommend the things we do – shows them that there is hard data behind the advice. When we can back up our advice with facts, we help ourselves and the people we advise by helping them make informed choices.

Erich Samuel is a Senior Information Security Consultant at a large global insurance company.

SOURCE Barcelona 2010

A Global Security, Business, and Technology Forum

September 21st-22nd, 2010
Museu Nacional D'art de Catalunya, Barcelona, Spain

www.sourceconference.com

USE DISCOUNT CODE

'SOURCEHN10'

To Get 15% Off Your Ticket Price!

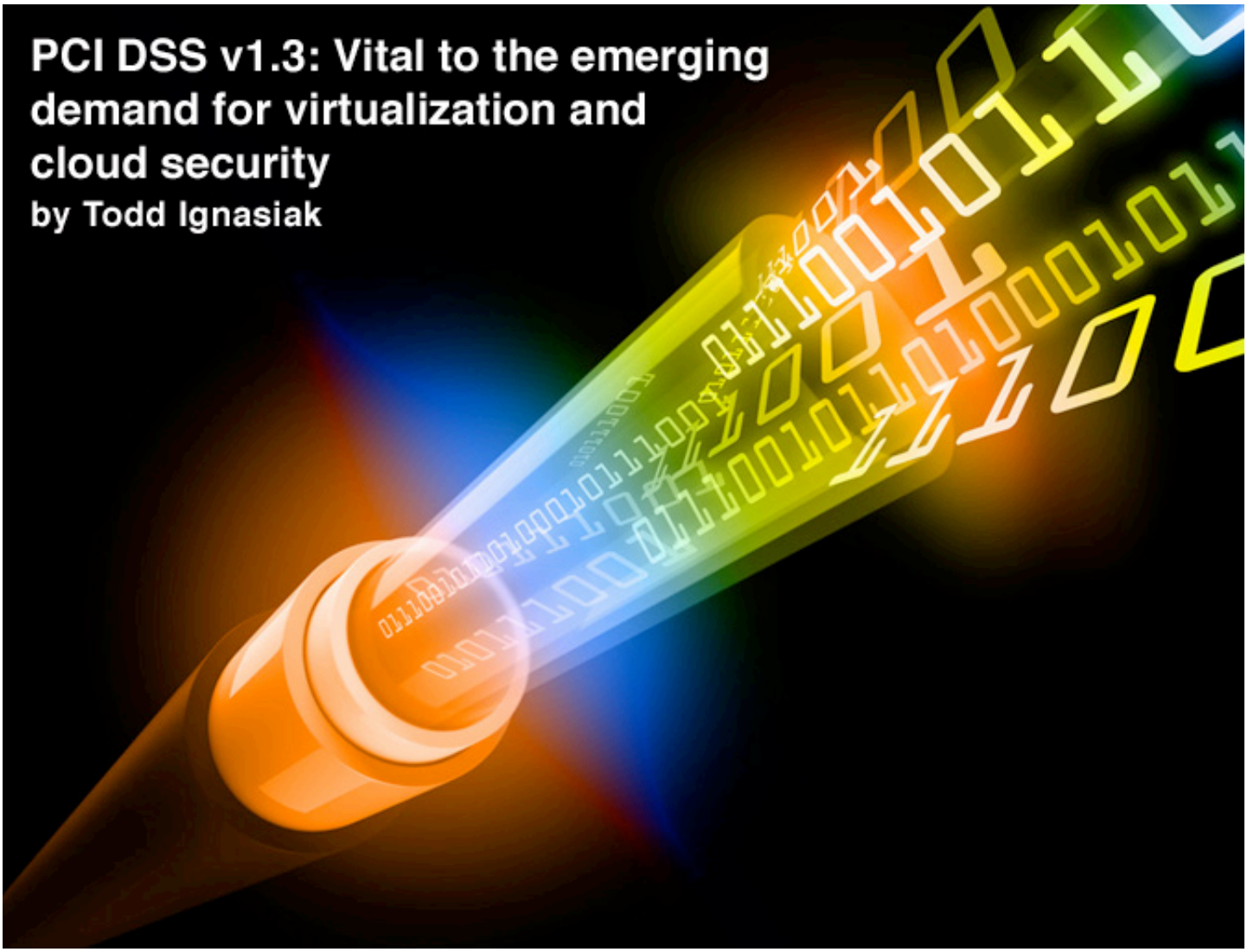
Exclusive Access To Speakers
Networking Events
Conference Party
Anti-Virus Workshop

Speaking Topics Include:

Breakthroughs In Challenging Technologies
Hacking And Consulting Tools Releases
Realities Of The Underground
Business and Technology Synergies
Proof-Positive Live Demonstrations
Vulnerabilities and Exploit Research
Problem-Solving For The Real World

PCI DSS v1.3: Vital to the emerging demand for virtualization and cloud security

by Todd Ignasiak



If you're part of the quintessential IT personnel most firms have, you've already had some exposure to virtualization technology. In all likelihood, portions of - if not your entire testing and development environment - run on a virtualization platform from VMware, Microsoft or Citrix.

The savings in capital and operating expenses are so compelling that now you've been asked to expand virtualization's use to the rest of your data center, demilitarized zone and disaster recovery site - basically, any other part of the physical network where migration of physical servers to virtual machines (VMs) will trim down the costs to power, cool, house and administer them. In fact, the likelihood that you have already embarked on such an effort is pretty high.

In a Gartner webinar, analyst Thomas Bittman said that "by 2013, the majority of workloads running on x86 architecture servers in enterprises will be running in virtual machines."

This statistic implies that virtualization is quickly subsuming critical workloads, with valuable, sensitive and compliance relevant data and applications making their way onto VMs. The challenge presented stems from the fact that virtualization combines workloads of different trust levels (i.e. HR file server, CRM database, email server, etc.,) onto one physical server, and how can an organization remain compliant with requirements for the segregation of duties, zones of trust and least privilege access?

Furthermore, as virtualization adoption within organizations broadens to include dispersed data centers, so too does the use of live migration and automation - features which make it easy for VMs to be created and optimally operated but make it hard to continuously monitor and secure them.

Enter the PCI Security Council

The Payment Card Industry's (PCI) Data Security Standard (DSS) provides guidance on how to best protect payment cardholder information and transactions. While it does not mandate particular products, it does offer detailed information on how certain technologies may be used in this effort. For this reason it has long been lauded as the easiest to comprehend and implement of the regulations that constitute the compliance arena (e.g. SOX, HIPAA, Graham Leach Bliley, FISMA, and FERC). Unfortunately, the current version of PCI DSS, v1.2, does not address how to achieve its stated goals and protections within virtualized environments. This has created a lot of speculation and concern among organizations, especially when virtualizing their critical workloads where they are sacrificing a compliant PCI audit result.

While concerns about virtualization's risks within the context of PCI compliance abound, at the heart of the issue is Section 2.2.1, which states organizations should "implement only one primary function per server." This can be interpreted in a number of ways:

• If "server" indicates a hardware device, then all virtualized environments running VMs of different types (e.g. Web servers, databases) as guests on a single hardware host will be in violation of this requirement.

• If server denotes VM, then environments – which have the technical means to limit applications on a PER VM basis – will comply.

Therefore, the interpretation of requirement 2.2.1 for the virtualized environment becomes extremely important both for virtualization's adopters who are looking to maintain their PCI compliance and for qualified security assessors (QSAs) and auditors.

PCI DSS mission: To provide guidance for virtualization

In order to provide much-needed guidance, PCI formed a virtualization special interest group (SIG), which examined some of the issues and challenges posed to PCI compliance in virtualized environments. The group, which began meeting in the fall of 2008, brought together security vendors, practitioners, banks, merchants, auditors and QSAs, who have been meeting on a regular basis over the course of a year and a half in order to draft a recommendation for how the PCI DSS might be enhanced to include virtualization technology.

The SIG's work was leveraged by a PCI technical working group, which among other efforts has been drafting a mapping "tool" that will define the PCI DSS requirements in the context of the virtualized environment. The tool and other guidance which is slated for release in October of 2010 as part of PCI DSS v1.3 is extremely timely and absolutely vital to securing what is slated to become the de facto data center architecture. There are a number of reasons why the PCI technical working group's efforts are critical:

1. Some firms have gone forward with virtualization and as a result risk failing a subsequent audit. Firms are incurring the risk to their networks and they will be joined by many more as virtualization adoption explodes.

2. Auditors and QSAs have no training or experience in securing virtualized environments so there is no consistency to the audit process.

3. Cloud computing and cloud services adoption is soaring. And validating this trend are large scale virtualized data centers, that are likely the providers of Infrastructure as a Service (IaaS) to the small businesses and merchants who must maintain PCI compliance in order to be able to accept credit cards for payment.

Checklist: What can you do today?

Consider, for example, that you have virtualized a portion or your entire data center, or that a virtualization strategy is in process.

Ask yourself the following question: What can you do today to ensure that you pass your PCI audit? The following five best practices are key protection elements for any network. They form the basis for PCI compliance within physical networks, as well as for the virtualized network.

The five key tenets to PCI–compliant virtualized environments are:

1. Isolate/segment workloads or servers or virtual machines.
2. Isolate/segment networks or groups of servers or groups of virtual machines.
3. Protect server or virtual machine contents.
4. Log and audit all events including administrator activity.
5. Continuously monitor security against changes.

The following briefly describe each tenet and offer guidance on how they can be accomplished in the virtualized environment:

Tenet 1: Isolate/segment workloads or servers or virtual machines

Protecting cardholder data implies that if a server containing the data is compromised, that the risk is limited to that server alone, and not others who are logically or physically connected to it.

In order to ensure this protection, requirement number one of the PCI DSS is to "install and maintain a firewall configuration." In the physical world, this type of protection is provided by network firewalls. Rules are defined and enforced to limit traffic in and out of servers that contain cardholder data, sent to only known traffic sources and expected protocols. If for some reason the server becomes infected with a virus that attempts to spread itself, the unauthorized connection attempt will be blocked.

The same type of protection and isolation is possible with hypervisor-based firewall technology. Policies limit access to the virtual machine by application, protocol and port, ensuring that only authorized traffic sources can gain access. The underlying firewall technology is the same that is used to protect cardholder data in physical networks, but it has been optimized for performance and security in the virtualized environment. Employing a virtual firewall allows organizations to comply with PCI DSS requirement 2.2.1 – which calls for "one function per server" – without requiring that separate VM hosts be purchased for each in-scope VM or VM group.

Tenet 2: Isolate/segment networks or groups of servers or virtual machines

In addition to isolating individual VMs and ensuring warranted access, the same process must be applied to groups of virtual machines. This becomes particularly apt in the cloud hosting environment where the cardholder data bearing VMs of customer A must be segmented from those of customer B. Isolation of groups between virtual machines can be accomplished in a number of ways. One may choose to confine certain VMs to a given physical host. However, this can get expensive in larger deployments. Another common way is through VLAN segmentation where virtual switch and port assignments are maintained for certain groups of VMs.

This method is popular but becomes quite cumbersome to manage at scale where new VMs are created or introduced frequently. The challenge with the latter method is that errors and misconfiguration (i.e. a VM assigned to the wrong VLAN) are quite common. For best results, virtualization security experts should combine VLAN segmentation with virtual firewall technology. The former can enforce VM to VLAN assignment automatically so that that the risk to cardholder data posed by VLAN mis-assignment is virtually eliminated.

Tenet 3: Protect server or virtual machine contents

Just as in the physical world, cardholder data on VMs must be protected from prying eyes and possible theft. CSOs and security administrators need to take the necessary measures to protect the physical media carrying the VMs as well as securing the data at rest on the VMs. Encryption, which is put forth explicitly in PCI DSS requirement number two, is essential for this purpose as is multi-factor user authentication. The former should be applied at all layers, disk and data and to all instances of the VM, including backups. Also, strong authentication will ensure that only those administrators with the highest and appropriate privilege will be able to access cardholder data. Most virtualization platforms broadly support available encryption and authentication technologies, although verification of software version compatibility is strongly advised.

Tenet 4: Log and audit all events

PCI DSS requirement 10 sets forth that "all access to network resources and cardholder data be tracked and monitored". This must be conducted for all types of access including that of administrators. The types of events that should be logged in and for which there should be a readily available audit trail include: successful and failed login attempts, user and group access privilege changes, VM network assignments and changes.

Administrator login attempts and user privilege assignments can be readily tracked with tools available from the virtualization platform providers and the utilities of their management systems. VM lifecycle and network assignments can also be easily tracked in this way.

In order to create a complete picture of access activity, virtualization administrators will also want to implement "in-line" technologies like virtual firewalls which monitor and selectively log all traffic flows, access types, security rule matches. These devices will also monitor hypervisor access attempt activity. Use of virtual firewalls with integrated IDS will also provide an audit trail of authorized access inspecting all packets bound for in-scope servers for the presence of malware.

A complete audit trail of this sort can aid in troubleshooting as well as virtual network optimization in addition to providing data for forensic analysis and security policy refinement.

Tenet 5: Continuously monitor and manage against change

PCI DSS requirement six calls for "change control". In the physical world this is accomplished through products for patch management.

However, controlling the configuration of a VM is much more difficult. Since VMs can be created, cloned and otherwise configured with a mouse click it is very difficult for administrators to keep in-scope servers in compliance with the ideal or desired configuration. To accomplish this, virtual network administrators should consider deploying a combination of technologies, including VM introspection, automated compliance assessment and configuration management.

The former two allow for the automated detection and alerting of changes to virtual machines, including the networking settings as well as the installed applications and services. An automated assessment process can alert VM administrators when there are deviations or VM state changes that negatively impact the risk profile.

There are several commercially available solutions that leverage VM introspection for this purpose. Configuration management allows for rollbacks and updates to be conducted so that after detection, remediation of the VM state can be carried out quickly. There are many solutions available for configuration management and remediation for virtualized servers.

Conclusion

Not only is PCI compliance within the virtualized environment possible, but it may actually be easier and more cost-effective to achieve than it is in the physical network. While PCI DSS v1.3 will bring forth much-needed explanations of the requirements for the virtualized environment, the end goal of protecting cardholder data is the same, and the onus still falls to the end-user (i.e. businesses, organizations, security practitioners) to decide how to best achieve this goal.

The key to making the best possible choices is in knowing that virtualization has given rise to a host of purpose-built technologies that ensure security and compliance in an automated and dynamic fashion akin to the management of the virtual network itself.

Todd Ignasiak is the Director of Product Management at Altor Networks (www.altornetworks.com). He is responsible for product management and building the next generation of security to address the virtual data center. Ignasiak has been in the network security field for 15 years. Previously he created network security solutions for vendors including Check Point Software and secured large enterprise networks at Ford Motor Company. He is a member of the PCI DSS technical working group.

SOURCE Barcelona 2010 (www.sourceconference.com)
Barcelona, Spain, 21-22 September 2010.

Brucon 2010 (www.brucon.org)
Brussels, Belgium. 24-25 September 2010.

RSA Conference Europe 2010 (bit.ly/rsa2010eu)
London, United Kingdom. 12-14 October 2010.

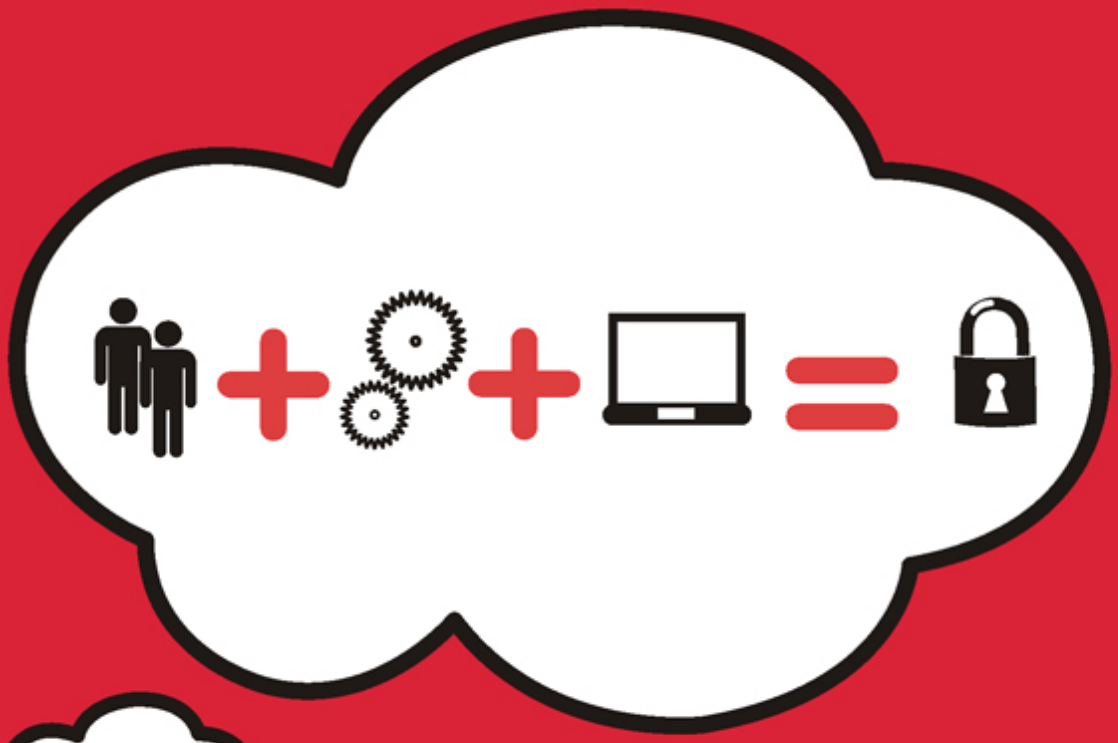
Gartner Security & Risk Management Summit (europe.gartner.com/security)
London. 22-23 September 2010.

2nd International ICST Conference on Digital Forensics & Cyber Crime
(www.d-forensics.org)
Abu Dhabi, UAE. 4-10 October 2010.

CSI 2010 (csiannual.com)
National Harbor, MD, USA. 26-29 October 2010.

GRC Meeting 2010 (www.grc-meeting.com)
Lisbon, Portugal. 28-29 October 2010.

RSA Conference 2011 (rsaconference.com/helpnet)
San Francisco, USA. 14-18 February 2011



INFOSECURITY RUSSIA. STORAGE EXPO. DOCUMATION'2010 – RUSSIA'S PREMIER EVENT

The VII-th International Exhibition InfosecurityRussia. StorageExpo. Documation'2010 ensures maximum usefulness of the visit for attendees and the highest ROI in Russia for exhibitors.

Register free to attend now at:
www.infosecurityrussia.ru

The premier event for the markets of information security, data storage, electronic document management and state electronic services in Russia.

17 – 19 November 2010

Sokolniki Expo & Cultural Centre, Hall 4

Moscow Russia

infosecurity RUSSIA

STORAGE EXPO

DOCUMATION

Organised by:
Groteck Business Media

Security testing - the key to software quality

by Rob McConnell

The IT security landscape has changed dramatically over the last few years. Low entry barriers and high rewards have induced many criminal organizations to try their hand at cyber crime. Large-scale attacks such as those perpetrated against Google and 30 other U.S. companies in early 2010 are a proof that the security battle is still very far from being won.

In addition to that, an ever-increasing number of regulations see to it that enterprises now take more responsibility for their digital actions than ever before. Compliance is a key driver in many security sectors. And though most companies try to protect their information and computer systems in good faith, many have failed to commit the resources and expertise necessary during all phases of system development and implementation.

Security management is key

Overall security policy and management is often at the root of security problems. Recent years have seen the promotion of international standards for IT security management such as ISO27001, but mainstream adoption has not been widespread.

It is of vital importance to make security a prominent consideration before, during and after any IT system implementation or upgrade, and every organization should have a comprehensive plan in place for addressing security issues during every phase of an IT project: conceptualization, design, development, test, rollout and maintenance.

Many of today's organizations do not have enough resources to invest into strategic security planning and management, so they simply implement or maintain a system that works. This is often due to lack of money, but can also be a case of lack of education. It is clear that there is an inconsistent approach to how software and system security is addressed and managed, and this continues to fuel the numbers of IT security incidents making headlines.

The current cloud trend will likely affect this pattern. By outsourcing ICT requirements into the cloud, users are effectively transferring

the liability for their security risk via contract to the provider. This does not make the security issues go away, merely transfers the ownership of the problem.

Although, it is conceivable that the use of the cloud will take some organizations' security posture to a higher level than the one they are currently unable to achieve. Media pressure will also make consumers demand that security is addressed when adopting the cloud. Prospective adopters of cloud services should also take great care when investigating security guarantees and claims made by service providers.

However, even with the emergence of the cloud, it should be noted that the types of security threats facing ICT remain similar and that the control measures needed to address such threats have not changed significantly. A common requirement - regardless of the technology delivery mechanism - is security testing.

SECURITY TESTING IS A POPULAR, BUT OFTEN MISUNDERSTOOD CONCEPT

Security testing, trial and error?

Security testing is a popular, but often misunderstood concept.

At its most basic level, security testing is aimed at identifying security vulnerabilities and weaknesses in software and systems, in order to fix them before they can get exploited. Well-publicized examples include SQL injection and buffer overflow flaws. It's important to recognize that security vulnerabilities are not necessarily the product of poorly designed or coded systems. Many security vulnerabilities are the result of configuration errors in hardware and software, caused by human error during implementation or upgrade.

A good security testing strategy is an essential element of any security risk management plan, especially for mitigating minor human errors that can snowball into serious breaches if not identified early on. A strategy for testing and verifying all aspects of hardware and software integration is a 'must have' for any system implementation or software development project. It is also essential that such strategies broadly approach the matter of security, rather than focusing on specific 'high risk' areas such as authentication and access management. This ensures the identification of unexpected problems, as well as of those anticipated.

A common, cost efficient approach has been to develop and implement business systems first, and then follow up with a short black box penetration test to see if the system can be penetrated. However, this leaves systems wide open to attack because other areas are neglected.

This problem can be solved by raising awareness of the fact that there are other security tests out there, and that a more consolidated, comprehensive approach to security testing across all the components of today's business systems is needed.

It simply makes sense to start testing as early as possible in order to avoid potentially critical vulnerabilities sneaking into mission critical systems. Advances in technology make it so much easier for security testing to be integrated alongside traditional testing programs - automated tools for source code analysis and simulation of web-based application-level attacks enable the discovery of security issues before the production phase. However, automated tools have their downsides (e.g. false positives) and should always be complemented with manual testing.

HP's and IBM's drive to acquire security testing technology should be seen as a proof of the increased importance and awareness of the need for broader security testing efforts.

With that in mind, IBM has acquired Watchfire and Ounce Labs in 2007 and 2009, respectively.

“Secure applications are vital to information integrity and continuity in government and business,” commented Daniel Sabbah, general manager of IBM Rational software.
Given that many security weaknesses are the result of errors or misconfigurations, it is also essential that security testing covers the configuration testing of key components of IT systems, from network devices to databases and applications.

It's also vital that testing does not just stop once a system has gone live. A continuous security testing process is required, and it must involve the full range of test activities, from automated vulnerability assessments to manual penetration and configuration checking techniques.

OFTEN LAID AT THE DOOR OF THE IT DEPARTMENT, SECURITY RESPONSIBILITY HAS NOW MOVED OUT OF THE BASEMENT AND INTO THE BOARDROOM

QA for peace of mind

Historically, an often casual approach to security testing has been used when compared to testing of other non-functional software and systems. This can be partly attributed to confusion over the ultimate responsibility for security functions within an enterprise. Often laid at the door of the IT department, security responsibility has now moved out of the basement and into the boardroom, with an increasingly strong drive from compliance obligations.

As stated, the broadening of the cloud services marketplace will drive a transfer of ownership, which will make companies adopt a wider focus on security in general. It is also possible that cloud users will seek some form of security certification (e.g. Kitemark) that demonstrates that the service provider is committed to security.

The days of conducting penetration-style testing and running some open source vulnerability analysis tools on an ad hoc basis are long gone, and the need for stakeholders to collaborate and share responsibility for an effective security testing strategy has never been higher.

Regardless of the ICT solution or delivery model, security is synonymous with quality software, and companies that strive for stability and scalability in their ICT solutions must put equal emphasis on security.

The security risk profile of software and systems has changed, and although a moving target, it still needs to be addressed in a layered fashion. A formalized approach is therefore required, involving collaboration across organizations and enterprises, and definitely including a rigorous testing procedure.

Security testing fits firmly into the discipline of software quality governance and is included in an overall security policy stance that most enterprises should aspire towards. Without placing due importance onto security testing of both new and existing systems, businesses are liable to increase their exposure to unstructured risk.

Rob McConnell is a Market Director within SQS Group (www.sqs-group.com), having spent the past 15 years specializing in the field of information and systems security management. Rob holds industry recognized security professional qualifications including CISSP, CESG Listed Advisor and ISO27001 Lead Auditor.

Oops!Backup (www.net-security.org/software.php?id=783)

Oops!Backup is an extremely easy to use CDP (Continuous Data Protection) backup for Windows 7, Vista & XP (64 and 32 bit). It's fully automatic and can go back in time to restore different versions of backed up files.

TCPView (www.net-security.org/software.php?id=319)

TCPView is a Windows program that will show you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.

The Sleuth Kit (www.net-security.org/software.php?id=215)

The Sleuth Kit is a collection of UNIX-based command line file system forensic tools that allow an investigator to examine NTFS, FAT, FFS, EXT2FS, and EXT3FS file systems of a suspect computer in a non-intrusive fashion.

BestCrypt (www.net-security.org/software.php?id=173)

BestCrypt data encryption systems bring military strength encryption to the ordinary computer user without the complexities normally associated with strong data encryption.

Bulletproof Public PC (www.net-security.org/software.php?id=753)

Bulletproof Public PC will let you turn your PC into an Internet kiosk/public access workstation. It can be setup to completely disable access to files installed on your PC while giving full access to all necessary applications you specify.

the adventures of

alice & bob

RSA CONFERENCE 2011

FEBRUARY 14-18 | MOSCONE CENTER | SAN FRANCISCO

20 YEARS

Protect your business from malicious characters.

Join us as we celebrate the 20th anniversary of RSA® Conference.

Gain insights
Choose from 210+ sessions targeting today's security challenges.

Go in-depth
Dive into a variety of topics with 15 targeted program tracks.

Strengthen your network
Connect with peers and speakers—information security's best and brightest.

Refine your tools
Discover cutting-edge technologies and innovative solutions from 350+ companies.

Early Bird Savings

SAVE $700

when you register by November 19

Follow the Adventures of Alice & Bob at
www.rsaconference.com/alice&bob

Register early and save. Go to www.rsaconference.com/helpnet

A brief history of security and the mobile enterprise

by Winn Schwartau

IT architecture is a never-ending exercise in migration - a centric vs. non-centric flux that can never seem to make up its mind. And for decades, security - most assuredly the bastard step-child of IT - has been left to flounder and wildly twist in the wind, at first forgotten or ignored, but nonetheless tasked to clean up the mess that the IT folks have rendered.

The modern enterprise is now facing unprecedented threats and risks to its dynamic mobile infrastructure. This is that story.

Some of you might remember the 1950s. Doris Day and Cary Grant in a Big Blue computer room, paper-spewing and chaos ensuing. Not much security as massive 5MB disk drives, tape cabinets and consoles that ate punch cards by the pound, sequentially processing batch after batch of programs with no emulators to test them ahead of time.

Computer security was dogs, fences and teenage soldiers carrying M-16s to keep potential intruders from entering hyper-paranoid facilities such as nuclear weapons testing labs and the government's real version of the WOPR from War Games.

In the 1970s the United States Department of Defense labeled Cold War threats as paramount to national security. The 193 Bell-La Padula security model set the foundation for decades of information security, but does not work well for the distributed mobile workforce and the enterprise.

IBM's mainframe monopoly resulted in arguably the first software security product, RACF (Resource Access Control Facility) that provided authentication, authorization (access control) and auditing capabilities.

Security was comparatively easy. Hundreds or thousands of users were physically hard-wired to the data center (pre-IP of course). Products like RACF identified users with simple user_IDs and passwords, and the mainframe knew where every terminal was located. Users and groups of users were given access rights to specific files and directories. All of the intelligence was at the central processing unit, located in some distant environmentally controlled room.

On August 12, 1981 along came the 5150. You might know it better as the IBM PC. IBM's thinking was that this miniature 'almost a computer' was the perfect way to get small businesses addicted to IBM and would then grow into their larger offerings.

But business had a different idea. Why shouldn't they be able to run software locally on the PC and connect to the mainframe? With programs and data now being processed and stored locally at the PC, the old security rules and architecture had changed almost overnight.

Companies had to develop ways to manage distributed computers, and push out security policy and enforcement to the PC.

With the introduction of Local Area Networks, vendors introduced competing and incompatible products, with negligible standards.

With the introduction of Local Area Networks, vendors introduced competing and incompatible products, with negligible standards. From a security standpoint, the landscape changed again. There was no longer any need to run complex software at the PC. The LAN would manage it all, and your PC would not be burdened with the taxing processing.

This fundamental architectural shift in the IT industry again challenged us "security folks," as now we had to consider how to secure the LAN, the servers and the data that could still be stored on the PC. We were treading on entirely new ground.

In the rush to capitalize on Gordon Gecko's "Greed is Good" mantra so loved by the financial industry, along came client-server architecture. This architecture expanded on the LAN model by distributing processes and storage across a plethora of servers in an effort to increase power and balance loads. The business units demanded the function, IT built a solution, but the security problems were immense and never adequately solved. A hybrid of centralized, yet distributed security failure points, was a catastrophe until a savior appeared on the scene.

The sudden appearance of the Web triggered the development of yet another IT architecture. Every machine could be a client. Every machine could be a server. Not quite what we have come to know today as P2P networking, but certainly an early evolutionary step. Again, security was, at best, a minor afterthought since the Web was designed to be platform-agnostic.

Herein again, the mistakes of the prior generation of IT management were repeated with historical ignorance and arrogance. Let's take this phenomenal connectivity, build piles of cool applications that can be run on almost any computer from almost any computer, and return the power to the user.

Business was driving IT to build out function, secure web programming was a distant formalization, and the consumer demand was and is still, insatiable. Where does security fit into this model? Viruses, worms, and an endless supply of threats created a multi-billion dollar industry that is akin to the carnival game of Whack-a-Mole.

Fast forward to today: Given the consumerization of the Internet, security is again treading in untested waters. Servers need to be secured, but unless the virtual drawbridges are in the 'down' position, commerce is shut off. An architectural dilemma to be sure, compounded by the fact that this security model assumes that the individual user knows how, and will actively participate in the security process.

Expecting the home user, kids, parents and everyone else to abide by the best practices needed to protect themselves or their online activities was another exercise in hubris by the IT community. With the incredible growth of intelligent mobile devices replacing conventional computers counting in the hundreds of millions, history repeats itself, and we have valuable lessons that can be applied.

Software grew with exponential complexity and complexity breeds vulnerability, which in turn, breeds poor security. Consumers want function, but they need simplicity – which was not delivered until recently with the iPhone and similar devices.

Smart phones are the new computers. They are highly portable, increasingly powerful with a user base growing at double-digit rates. An estimated 2 billion of them will be deployed globally by 2013. Smart phones are computers that happen to have a telephone in them; they are used for traditional data-oriented computer tasks like email, surfing, data storage and business applications.

If there is a lesson has been learned in the last three decades, it's that security must have a balanced role with business requirements and IT implementation.

Unleashing vast amounts of sophisticated technology to hundreds of millions of people who have already proven that they are either incapable of or unwilling to take the appropriate security steps or adapt proper behavior to protect their identity, is a distinct threat to the enterprise and global security.

While to the user smart phones and notably the iPhone family are intuitively easy to use, the risks to the devices, their users or the companies that use them for business are, as with past technology innovations, afterthoughts. Security has – as always - fallen into the abyss of invisibility due to apathy, arrogance or ignorance.

We know that smart phone applications are the greatest tool ever devised to deliver hostile software to a computing device, and as of 23 June 2010, a study suggests that 20% of Android applications could be spyware. We know the iPhone has been rooted and there is an increasing library of hostile mobile code in addition to the applications. We also know that the bad guys are going to use and abuse any technology to their advantage, no matter the motivation.

We are also keenly aware that companies would dearly love to adapt the consumer iPhone and other smart phones for internal corporate applications. The healthcare industry wants to allow nurses and doctors to have the needed information, anywhere and anytime.

The retail industry wants to use these devices for virtual 'show and tell' shopping and mobile payment terminals. Every company wants to enable staff to access and utilize corporate resources.

The IT architecture that smartphones utilize is a hybrid of communications technology and IP technology, and the conventional security approaches of the past thirty years are incapable of addressing the mobile and smart phone security storm.

If there is a lesson has been learned in the last three decades, it's that security must have a balanced role with business requirements and IT implementation. However, smart phones cannot support the multi-tasking needed, CPU resources and bandwidth required, or the incessant battery drain such an approach would require – even if it could work.

Because, at the end of the day, these consumer devices allow the user to turn off every security switch if they so desire. That risk is unacceptable to any organization that must adhere to governance guidelines, compliance regulations and afford proprietary data protection and privacy.

The mobile IT architecture is completely unsuited for any heretofore-existing security model and securing the mobile workforce requires a fundamentally different security architecture that solves several, seemingly contradictory goals:

• It should have zero impact on the performance of the smart phone.
• It should be invisible to the user, who should not be able to bypass any controls.
• The enterprise should be able to mange many different types of smart phones with a single management, enforcement and control console.
• Existing corporate security policies should be easy to migrate to any entire smart phone population in a few hours.
• It should meet best security practices and compliance requirements of many industry sectors.
• Any business should be able to design and deploy applications without having to worry about the complexities of secure programming as is needed even with web applications.

Any business should be able to design and deploy applications without having to worry about the complexities of secure programming as is needed even with web applications.

The mobile security problem is not going away because we wish it to. In fact, it is more complex than ever before and the sheer number of users is driving the consumerization of IT and the proliferation of these dual-use devices faster than any technology in history.

The control of computing devices has migrated from the centric to the non-centric and back. The intelligence of devices has similarly moved from point to point within the IT infrastructure and the response of the security industry to the hyper speed of technology innovation and deployment must accommodate the new mobile requirements of business, government and the consumer.

I invite readers to consider one approach to this massive problem: moving all security controls and enforcement off of the internal enterprise, the end point devices, the desktop and into a secure 'halo' where security comes first and application comes second.

Imagine: a private security cloud where the business guys can actually design applications with minimal restrictions. Imagine: a single administrative and control point for the mobile enterprise.

There is no need to imagine that this is real - because it is.

Winn Schwartau is Chairman, Board of Directors, Mobile Application Development Partners, LLC and consults with private and government organizations around the world. He is an expert on security, privacy, infowar, cyber-terrorism and related topics. Schwartau has testified before Congress, advised committees and has consulted as an expert witness.

Join Us

GRC Meeting 2010

Governance, Risk & Compliance

The Meeting Point for IT Managers in Portugal

28th and 29th October 2010 - FIL, Parque das Nações, Lisbon

GET MORE AT WWW.GRC-MEETING.COM

THE EVENT

The GRC Meeting 2010 aims to bring to participants, the main challenges that managers involved in the areas of IT Governance, Risk & Compliance has, in order to also share strategies, solutions and methods best suited to deal with such challenges before, during and after the global economic crisis.
With over 20 activities, 2 days' duration, with speeches and workshops that should add value to the business of the participants.

MACRO THEMES

- Security Awareness and Strategy;
- Risk Management;
- Identity Management;
- Business Continuity & Disaster Recovery Planning;
- Auditing & Standards;
- IT Governance and Risk Management;
- Web 2.0 and the Impact on Enterprise Security;
- Data Privacy;
- Cloud Security Computing;
- Identity Theft.

KEYNOTE SPEAKERS

Bruce Schneier
Chief Security Technology Officer of BT

Danny Lieberman
Managing partner and principal consultant at Software Associates

John P. Pironti
President of IP Architects, LLC

John Howie
Senior Director of Technical Security Services, Global Foundation Services of Microsoft Corporation

Geraint Price
Royal Holloway University of London - Identity Management

Anderson Ramos
CTO and founder of FlipSide Smart Content Provider

Samuel Sadek
Corporate Information Risk, Compliance and Security Management Professional

SAVE 20%: exclusive for (ISC)2 associates

Sponsors

Media Partners

Co-Marketing

Transport

Organizer

In Cooperation With

The PCI Data Security Standard mandates foundational controls, most of which are information security best practices. It is a one-size-fits-all standard meant to address all business and technological environments that store, process or transmit payment card data. Minimum compliance with PCI standards may not adequately protect card data. It is, therefore, necessary to conduct a risk assessment in accordance with PCI requirements.

Organized crime is in the business of breaching card data and committing fraud to profit from their efforts. Business is booming and they are reinvesting. The level of sophistication is apparent. One recent breach was identified by common point of purchase fraud analysis. It took two forensics teams to find the source of the compromise. Sniffer malware was installed on an unassigned section of a server hard drive, outside of the operating system. Hackers are also using malware to collect unencrypted card data stored in system memory.

Professional hackers are innovative and patient. They slowly infiltrate an environment, learn how card data flows and subtly probe for vulnerabilities. They create custom malware unique to the IT environment and test against anti-virus software to avoid detection. Next, they install the malware and exploit the payment application. Once card data has been collected, hackers encrypt it and use anti-forensic tools to further avoid detection. Highly difficult attacks accounted for 95% of all compromised records (bit.ly/BWNI4). Be mindful of the threat posed by authorized personnel. In addition to malicious insider threat considerations, internal personnel may introduce vulnerabilities through human error. A malicious actor may assume the guise of an employee through a technological exploit or compromise them through social engineering.

I. Management support

Resources are required to conduct a comprehensive risk assessment. Explain the current threat landscape to senior management. Determine their risk tolerance and request their active support. Assign a dedicated function to conduct risk assessments to establish accountability. In a small organization, it may be an alternate duty for a security professional. In a medium sized organization, consider hiring a full-time security professional. In a large organization, a small team should be dedicated to technology risk assessment. It will be necessary to involve members of multiple teams to conduct the risk assessment. Consider establishing a project to identify participants, conduct the assessment and finalize remediation.

II. Data flows and systems

Create a data flow diagram that documents where payment card numbers are stored, processed and transmitted. From the PCI Data Security Standard, diagrams should detail physical and logical data flows, "including transmission and processing of card data, authorization, capture, settlement, chargeback and other flows as applicable" (bit.ly/b7di9). As a best practice, scan for payment card data outside the PCI environment at least annually.

Next, establish an inventory to document the systems, applications and databases associated with each PCI environment. Include details such as information owner, data custodians, application managers, PCI network scans and when the last application assessment was conducted.

Card Brand	Comments	Regular Expression
Visa	All Visa card numbers start with a 4.	^4[0-9]{12}(?:[0-9]{3})?$
MasterCard	All MasterCard card numbers start with numbers 51 through 55.	^5[1-5][0-9]{14}$
American Express	American Express card numbers start with a 34 or 37.	^3[47][0-9]{13}$
Discover	Discover card numbers start with 6011 or 65.	^6(?:011|5[0-9]{2})[0-9]{12}$

Source: PCI Security Standards Council.

III. Risk and control assessments

PCI requirement 12.1.2 includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. To identify threats and vulnerabilities, subscribe to US CERT advisories, the DHS daily cyber report and vendor security alerts. Merchants can obtain the Visa list of vulnerable applications from their acquiring bank. Information security professionals should join the U.S. Secret Service Electronic Crimes Task Force and FBI InfraGard. ECTF and InfraGard are free and provide threat and vulnerability advisories.

The scope of a PCI risk assessment is the same as that of a PCI assessment. Follow the flow of payment card data in production and disaster recovery environments and evaluate compensating controls. Conduct a thorough risk assessment before implementing new technologies such as virtualization or cloud computing.

Conceptualize data flow as a pipe with holes in it. Areas of vulnerability include systems between encrypted network connections and the data flow channel itself such as application security attacks that easily pass infrastructure security controls.

IV. Failure Mode and Effects Analysis

Failure Mode and Effects Analysis (FMEA) is a method used to evaluate potential failures within a process or system. Analysis includes consideration of failure severity, rate of occurrence and detection. FMEA was introduced in the 1940s by the US Armed Forces. Later, it was adopted by NASA, the Ford Motor Company and most recently, Six Sigma (bit.ly/KZvHY).

FMEA is also a practical way to conduct a technical risk assessment (bit.ly/cD80M2). Depending on the size and complexity of the environment, it will take between eight and sixteen hours to conduct an FMEA evaluation. In large organizations, maintenance of controls may be assigned to several teams.

FMEA participants should include representatives from physical security, system and network administration, application development, information security and operations.

System Component	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s) of Failure	Occurrence	Current Process Controls	Detection	RPN

System Component: Evaluate each system component listed on the card data flow diagram such as routers, firewalls, servers and point of sale systems.

Potential Failure Mode: For each system, determine how card data could be compromised at physical, network, host and application layers.

• Physical: Consider how card data could be stolen in-person such (e.g. by taking a server from a computer room).
• Network: Consider how card data could be compromised in transmission over the network (e.g. by using sniffer software).
• Host: Consider how card data could be compromised while in storage or while in system memory (e.g. by using malware or a zero day attack).
• Application: Consider how card data could be compromised at the application layer (e.g. by exploiting a software coding error).

Potential Effect(s) of Failure: Describe the consequences of the failure mode such as payment card data being compromised.

Severity: Enter a numeric rating associated with the severity of the failure mode.

Potential Causes of Failure: Describe potential causes of the failure mode.

Occurrence: Enter a numeric rating to represent the probability of the failure occurring.

Current Process Controls: Describe existing controls that detect or prevent failure.
Detection: Enter a numeric rating to represent the probability of the failure being detected.

RPN: Risk Priority Number = Severity X Occurrence X Detection.

Use RPN scores to prioritize remediation. The highest RPN values correspond to issues with the greatest potential for business impact.

V. Risk assessment scenario

In this scenario, a large corporation used FMEA to conduct a thorough risk assessment of their PCI environment. Senior management, in partnership with information security and audit, defined the following problem statement: The PCI Data Security Standard (DSS) is a publicly available control baseline. Organized crime syndicates and their hackers are familiar with it. The complexity of an IT environment makes it difficult to maintain in practice. For these reasons, it is necessary to conduct a thorough analysis of the cardholder data environment to determine where opportunities to compromise data are present. This approach is also in keeping with the PCI requirement for an annual risk assessment. As a result of FMEA evaluation, the following recommendations were made to mitigate risk above and beyond PCI DSS requirements:

Preventive controls:

Preventive controls are necessary to protect card data from compromise. Each control environment is unique and compliance with PCI requirements alone may not be sufficient to mitigate the risk of compromise.

Restrict cardholder environment access to company-owned computers. Requirement 1.4 permits employee-owned computers to connect to the cardholder data environment. Employee-owned systems are outside of the control of employers and cannot be subjected to systematic removal of accesses from a payment card data perspective.

Encrypt data over private, internal networks. Requirement 4.1 addresses encryption over open, public networks, stopping short of requiring encryption over internal networks. There has been a trend of data compromises where card numbers have been compromised over unencrypted network connections.

Relying on perimeter security alone is akin to “candy security”, hard on the outside and soft and chewy on the inside.

Use firewalls to segment card data from internal networks. The entire company network has connectivity to systems that store, process or transmit cardholder data, which results in costs associated with maintaining controls and assessment activity in accordance with PCI requirements. Segmenting card data from unrelated systems takes them out of the scope of PCI compliance, reducing risk of compromise and the cost of compliance.

Further restrict payment card network connectivity and traffic flow to protect card data. Eliminate the practice of passing full 16 digit card numbers to the marketing server. Truncation is a viable alternative, deleting all but the first six and last four digits. Network connectivity exists between stores, without a supporting business requirement. Restrict store network connectivity to the corporate data center.

Require customers to enter their zip code at unattended payment terminals. Requiring a zip code to process a transaction is a method to prevent fraudulent transactions. For additional details, research the Address Verification System.

Detective controls:

If a breach occurs, it is necessary to learn about it early to contain the incident and minimize business impact.

Implement configuration monitoring software to ensure system hardening remains in place, in accordance with industry best practices. PCI requires system configuration standards to be applied with file integrity monitoring to ensure configuration files are not altered without the system administrator's knowledge (requirements 2.2.c and 11.5 respectively). File integrity monitoring does not evaluate whether a system is appropriately hardened against attack.

Implement log monitoring software to detect security events. Log harvesting, parsing, and alerting tools are listed as optional for monitoring logs in requirement 10.6. It is not practical to conduct manual log reviews daily. In a recent report, 66 percent of victims had sufficient evidence available within their logs to discover the breach had they been more diligent in analyzing such resources (bit.ly/BWNI4). Implement log monitoring software and a process to ensure alerts are monitored and responded to.

Include a testing component to evaluate comprehension of security topics and policy. Requirement 12.6.1.b addresses employee security awareness training upon hire and at least annually. As a best practice, test each employee's comprehension through the use of a questionnaire. A social engineering penetration test can be used as an alternate testing component.

Scenario conclusion

The above section is not intended to be an exhaustive analysis of PCI requirements. Instead, it is an example of findings from a risk assessment. Conduct feasibility studies for each FMEA recommendation. Determine the cost of a solution and technology constraints such as performance impact from encryption.

Management should be aware of inherent risk to make informed decisions before feasibility and cost decisions are made without their knowledge.

In this example, senior management had a low risk tolerance due to compromises in the industry and related business impact to the affected companies. In the risk community, the term Black Swan refers to events with the potential for severe impact to business and a low rate of occurrence (bit.ly/3zz8nG). Business continuity planning is an example of preparation for a Black Swan. Risk assessments are necessary under the same rationale.

VI. Provide guidelines for risk mitigation

When a risk assessment identifies a vulnerability that exceeds the risk tolerance of your organization, it is necessary to address the gap. Here is a listing of controls that mitigate risk above and beyond PCI requirements:

Implement two-factor authentication to restrict access to PCI systems from the internal network. Requirement 8.3 addresses two-factor authentication for remote access originating from outside the network. Use of the same technology internally helps prevent compromise from unauthorized personnel by minimizing the risk of password disclosure.

Implement Network Behavior Analysis (NBA) to detect unusual activity. NBA monitors for changes in established network traffic patterns. It is particularly useful for detecting malware or other malicious activity. NBA can detect if a system passes traffic to another system for the first time or when an unusually large file is transmitted. It can also send alerts

when a new protocol is used.

Use application whitelisting to protect against malware and viruses. Whitelisting allows authorized programs to run and blocks all others. It takes the opposite approach to signature based anti-virus software, which blocks known exploits. Whitelisting can effectively block polymorphic viruses, which change each time they run.

Use Data Loss Prevention (DLP) to prevent leakage of card numbers over unauthorized networks. Implement DLP at network choke points such as an Internet network connection. Use host-based DLP to detect card numbers stored outside of the PCI environment and to prevent data loss through USB flash drives.

Use Database Activity Monitoring (DAM) to monitor database queries for malicious activity. After establishing a baseline, configure DAM to deny requests for more than a certain number of card numbers. DAM also includes audit trail functionality and can record a history of queries.

Use tokenization to replace Primary Account Numbers (PANs) as unique identifiers. Tokens reduce the risk and cost associated with processing card transactions. PCI compliance requirements are tied to PANs. Tokenization can be used as an effective scope reduction technique.

Conduct an adversarial security assessment. Compliance is the first level of maturity. Risk management is the second. As a final level of maturity, conduct a thorough, unscripted, adversarial assessment that exceeds the PCI requirement for a penetration test. For example, use an elite information security firm to align techniques with organized crime resources. When a physical or technological barrier challenges core capabilities, engage additional resources to penetrate further. Conduct the assessment over a month or more. Include social engineering within the scope of the test. The above techniques may be cited as compensating controls, depending on the situation. Document optional controls as company guidelines for securing payment card data.

VII. Report and present

Consider each PCI environment with a focus on operational risk. Do not skew results of an assessment for financial or political reasons. A decision made at the business unit or line of business level can impact the organization as a whole in the event of a compromise. Transparency is warranted. Executives should determine risk tolerance and have ultimate control of the budget and funding.

Finalize the risk assessment report with empirical data to support development of a business case for funding. Refer to the ISACA Risk IT Framework for industry standard methods to communicate risk. Present findings to executive management, including ongoing remediation and plans for the next risk assessment. Funding for security enhancements should be deducted from the cost center associated with revenue for the related product or service.

VIII. Conclusion

In the years that follow, consider using an external firm with PCI experience to lead the risk assessment. Use of an independent third party helps ensure risk assessment is comprehensive, versus a "check the box" exercise. Rotate methodologies each year. For example, use a PCI Qualified Security Assessor one year and an information security firm the next.

Organized crime represents an Advanced Persistent Threat to PCI environments. It is impossible to secure payment card data with absolute certainty. Maintain compliance with PCI requirements and remediate risk assessment findings. There is severe reputational damage and financial impact associated with a payment card data compromise. Each organization must protect card data in accordance with business objectives. Failure is not an option.

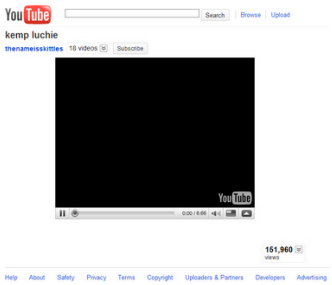
Gideon T. Rasmussen (www.gideonrasmussen.com), CISSP, CISA, CISM, CIPP is a Charlotte-based Information Security Manager with over 10 years experience in Fortune 50 and military organizations.

Infected flash drive blamed for US military breach

The most significant computer systems' breach in U.S. military history dates back to 2008, when malicious code contained in a flash drive infected a laptop of a military official posted in the Middle East, and spread further to the network of the U.S. Central Command. The code in question was put on the drive by operatives of a foreign intelligence agency, most likely Russian. (www.net-security.org/malware_news.php?id=1442)

Nearly 3 million undetected "Hot Video" pages pushing fake AV

We've seen many fake YouTube pages redirecting to fake antivirus software downloads in the past. However, we're now seeing this same phenomenon with a new twist: Google has indexed nearly 3 million "Hot Video" pages - all pushing fake AV. Yandex, a Russian search engine, also returns numerous links to these pages for random searches. The fake Youtube video page is covered by an invisible Flash layer and the Flash object automatically redirects the user to a fake AV page. If the user has Flash disabled, the page becomes harmless. The URL of the Flash file, hosted on a different domain, is obfuscated with Javascript. (www.net-security.org/malware_news.php?id=1441)

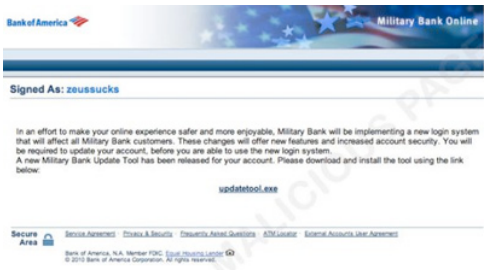


Malware peddlers engaged in celebrity mass killings

Plane crashes and car accidents are the preferred methods of killing off celebrities in order to lure email recipients into opening a malicious attachment. Beyonce Knowles, Brad Pitt, Jennifer Aniston, Johnny Depp - these are just a few of the names rotated in the template emails sent in this recent malicious spam run, professing that the celebrity in question was killed. (www.net-security.org/malware_news.php?id=1440)

U.S. military personnel targeted by malware

U.S. military personnel is targeted by cybercriminals. Fake email purportedly coming from Bank of America is asking holders of Military Bank accounts to update them by following the given link. According to Trend Micro, the link takes them to a very faithfully recreated bank login page, where they must enter their account username and password. (www.net-security.org/malware_news.php?id=1439)



Rogue AV uses legitimate uninstallers to cripple computers

The fact that some rogue AV solutions try to prevent the real ones from doing their job is widely known in the security community, but CoreGuard Antivirus - a "popular" fake AV solution - has been spotted utilizing legitimate software uninstallers to trick users into uninstalling their legitimate security software. (www.net-security.org/malware_news.php?id=1437)

ICQ worm spreads like fire

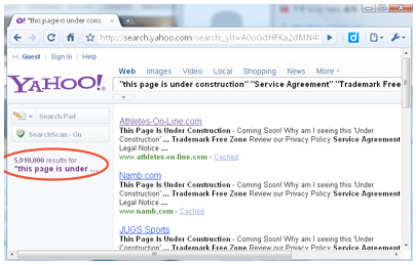
A new worm is targeting ICQ users, but apart from spreading itself by taking control of the ICQ application of the victim to send out more of the same messages and a file transfer request for an executable called snatch.exe, so far the worm does not appear to damage affected computers in any major way. (www.net-security.org/malware_news.php?id=1435)

Android game hides spying application

If you have a game called Tap Snake on your Android handset and you weren't the one who installed it, you are probably getting spied on by someone who had physical access to your device. (www.net-security.org/malware_news.php?id=1432)

5 million domains serving malware via compromised Network Solutions widget

A recent rise in the number of Armorize's customers' sites getting flagged by their own drive-by downloads and zero-day malware threats detection service HackAlert has led the the company researchers to the discovery of a compromised widget provided by Network Solutions.
(www.net-security.org/malware_news.php?id=1431)

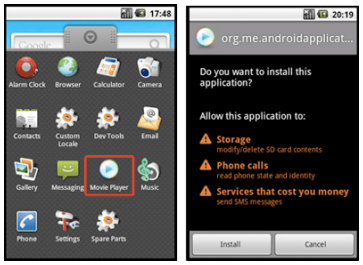


3,000 online banking customers robbed through targeted ZeuS attack

It took only a month to compromise some 3,000 private and business accounts with one of the largest financial institutions in the U.K. The criminals were able to leverage vulnerabilities found in the users' browsers and compromised websites in order to install Eleonore and Phoenix exploit kits into the machines, which only lead to a further installation of the latest variant (v3) of the well-known ZeuS Trojan. (www.net-security.org/malware_news.php?id=1430)

First SMS Android Trojan

The first SMS Trojan made specifically for smartphones running Google's Android OS has been detected by Kaspersky, and it seems that many devices have been infected already. The Trojan masquerades as an innocuous media player application and it misuses the Windows Media Player icon.
(www.net-security.org/malware_news.php?id=1427)

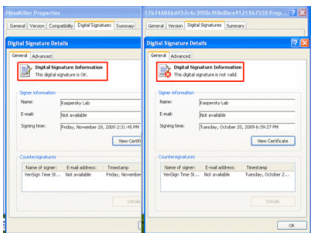


How can I know if my computer is infected? 10 signs of infection

Users are often advised to use an antivirus to check if their systems are infected, but with the current cybercrime scenario, this is not enough. It takes a least a basic grasp of security issues to work out if a computer is infected, and many first-time users have little or no idea. While many of today's threats are designed specifically to go undetected, there are still some tell-tale signs that a system has been compromised. (www.net-security.org/malware_news.php?id=1421)

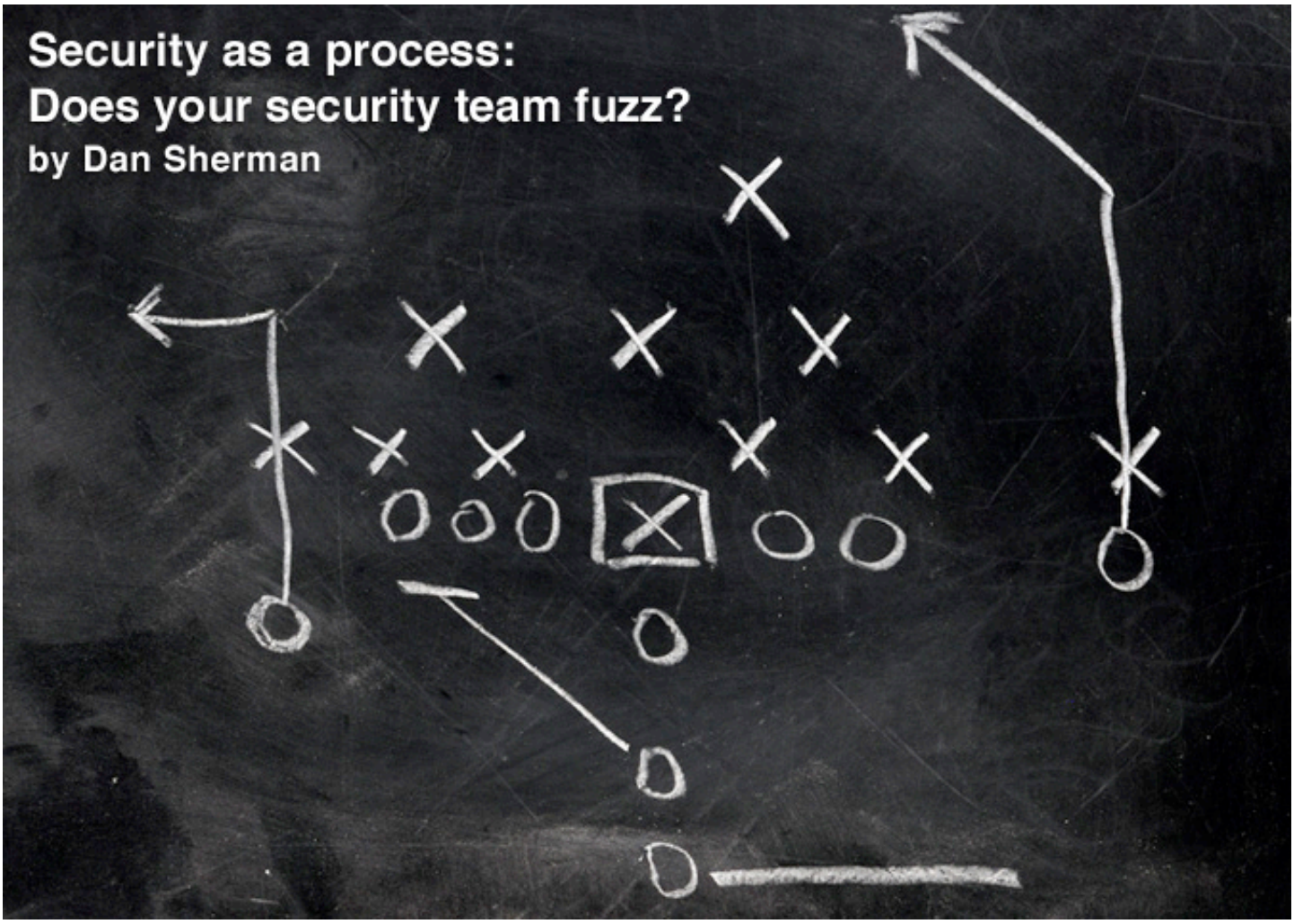
ZeuS variants hide behind snatched certificates

Copying certificates from legitimate files and mimicking signatures from certificate authorities is certainly not a new tactic in the cybercriminals' arsenal, but is one that seems to gain traction. The latest example comes from Trend Micro's researchers, who detected a bunch of suspicious files whose signature seemed to belong to Kaspersky, the well-known security company. (www.net-security.org/malware_news.php?id=1420)



Security as a process: Does your security team fuzz?

by Dan Sherman



Few days go by without news stories in which our nation's (un)preparedness to defend against cyber attacks is criticized. Though some criticism can be dismissed as political, the criticism of our nation's cybersecurity plan is fundamentally valid.

But, how can such an economically and militarily powerful nation be so ill-prepared to counter a large-scale cyber attack?

The answer is simple: the complexity of the cyber threat isn't fully understood by many high-ranking officials in both the government and private sectors. Either they don't comprehend the transformational nature of cyber warfare, or they don't understand the weighty ramifications of falling victim to an attack. As a direct consequence of this limited understanding, there are numerous existing guidelines and regulations that are either not enforced, or not enforced uniformly.

When cybersecurity first emerged as a discipline, it was focused on countering malicious attacks on large groups of users such as departments or institutions. However, with the onset of new technologies, the individual, rather than the institution, has become the new target for attack.

Vulnerable applications

As the number of smartphones and personal devices on any given network steadily increased over the years, so did the number of applications developed for those devices.

What was once a daunting task reserved for professional programmers, has now been simplified, allowing practical novices to develop and publish applications. And because amateur programmers are usually less inclined to include security into the development lifecycle, the increased number of application programmers has lead to an expanding number of vulnerable applications. Application layer attacks are also increasing in numbers.

Firewalls and operating systems usually get patched regularly, but the same thing cannot be said for applications. You only need to look at the number of instances of malicious PDF files being used to compromise computer systems, to know that this assertion is true.

Malicious links and the social Web

Application vulnerabilities are just the tip of the iceberg. Malicious links – especially those planted within social networking websites - are becoming increasingly difficult for the untrained eye to spot.

Cyber criminals are certainly taking advantage of these users. They use old attack methods but add to them the social component. The use of social engineering against targeted individuals has become the easiest and most efficient attack technique. Why? Because it is relatively simple to trick an untrained user into entering a website by clicking on a malicious link. And these links lead to websites where the user may again be tricked into entering personal information or opening a malicious file.

Reconnaissance

When a cyber criminal sets out to attack, he does some research first. This process usually starts with gathering information about the targeted company, or more specifically, its employees.

A basic web search allows the criminal to discover a wide range of information about an individual. A simple email address can lead him to a LinkedIn account, which may then lead to a social network account where an abundance of personal information can be found. This process continues until every piece of information that can be used to mount a targeted attack is discovered. The effective use of this information will allow the attacker to access the network and to start exploiting it actively.

Some cyber criminals also create hacking toolkits, which allow less technically savvy criminals to get their piece of the online action by hacking networks or creating a botnet with relative ease.

SOME CYBER CRIMINALS ALSO CREATE HACKING TOOLKITS, WHICH ALLOW LESS TECHNICALLY SAVVY CRIMINALS TO GET THEIR PIECE OF THE ONLINE ACTION.

Identifying vulnerabilities

Traditionally, companies have dedicated substantial resources to tactics such as penetration testing as a way to identify vulnerabilities that can be patched.

Although penetration testing is an important piece of the security puzzle, it is becoming much less important as time goes by and the need for a more fluid and flexible defense becomes apparent. Penetration testing is much like an incremental patch to fix a one-time problem; it is a static solution to a dynamic threat.

Changes in the cyber landscape demand that companies focus on security as a process, not as a one-time fix. Security must become an integral part of the development lifecycle. Penetration testing will still play a role in cybersecurity; however, it needs to be supplemented by additional measures such as source code audits, vulnerability assessments and fuzz testing.

Does your security team fuzz?

Fuzz testing, or “fuzzing,” is a term that was coined by Professor Bart Miller of University of Wisconsin, Madison, back in 1988. While he was remotely connected through his modem to the terminal of a Unix machine during a thunderstorm, he noticed that certain applications that he was executing were crashing due to the noise on the line - noise that he called “fuzz.”

At its most basic level, the act of fuzzing means taking an arbitrary set of data and putting it into a field. This process begins with a fuzzer, which injects the randomly generated data into an application input field or stream.

The intent is to send the unexpected data stream as input to determine how the application will respond. If the application crashes, testers know that there is a possibility that it is susceptible to malicious code execution.

Dumb or smart fuzzing

There are many types of fuzzers, but they can generally be categorized as either smart fuzzers or dumb fuzzers. For example, a dumb fuzzer will send random UDP write packets to a TFTP server, and then wait for the application to crash.

A smart fuzzer is a bit more involved. It sends a challenge, waits for a valid response, builds the next packet, sends it back to the server, has an agent to log the crash, memory dump, packet dump, and then restarts the entire process from the beginning. The smart fuzzer also has the capability to analyze the crash to determine if the possibility for code execution exists.

Fuzzers - smart or dumb - are relatively easy to run. However, the smarter they are, the longer they take to write and configure - especially if you want maximum coverage.

Why is fuzzing useful? It is useful because you normally don't have access to the source code and you gain the capability of finding vulnerabilities without reverse engineering or trying to decompile the application.

THE CYBERSECURITY PUZZLE HAS MANY PIECES, AND IT SEEMS THAT AS SOON AS YOU THINK YOU HAVE COMPLETED THE PUZZLE ANOTHER THREAT EMERGES. IF THAT'S THE CASE, THEN THE CYBERSECURITY PUZZLE CAN NEVER BE COMPLETED.

For example, many websites require a username and password combination to activate specific user account information. Both the username field and the password field are expecting a certain number of characters to be validated in order for the user to proceed.

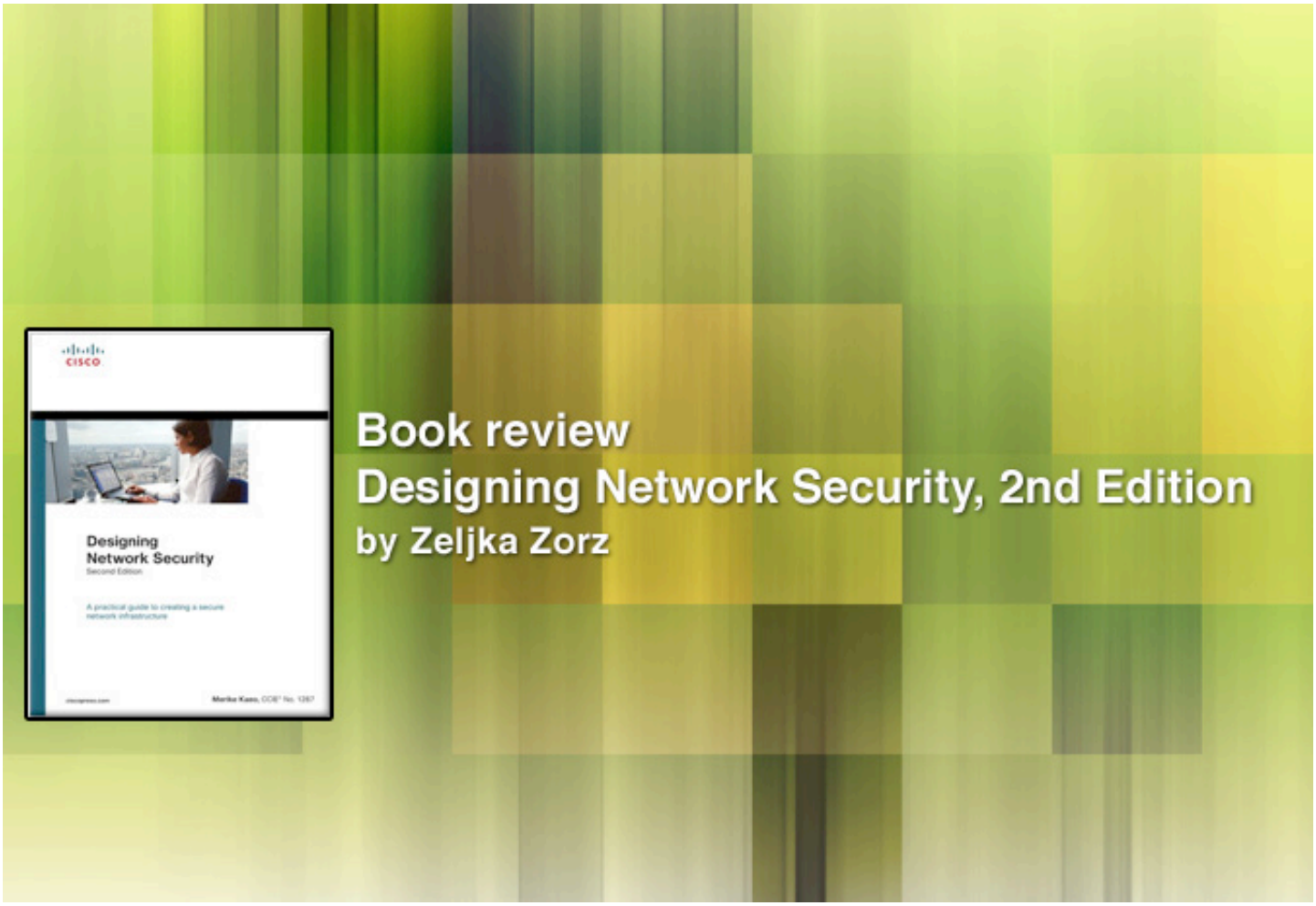
If you were to subject this application to fuzz testing, you could send a string of 30 "A"s into the username field. This field may not be expecting 30 "A"s, and could possibly cause a crash. It is possible to also send JavaScript tags while fuzzing, which would enable you find a SQL injection, or cross-site scripting attack.

Many developers use JavaScript to validate the fields of input on a website in order to restrict the user from entering more than a set number of characters. However, this restriction is easily bypassed and should not be used as the only form of input validation. The threat to web applications via SQL injection or cross-site scripting will only become more prevalent in the coming months and years.

The cybersecurity puzzle has many pieces, and it seems that as soon as you think you have completed the puzzle another threat emerges. If that's the case, then the cybersecurity puzzle can never be completed.

With that in mind, it is important to have a plan for a quick recovery, along with the ability to maintain the integrity of the data you are trying to protect. Because, in today's cyber world, it is not a matter of whether you will be penetrated - it is a matter of when.

Dan Sherman is the information assurance research lead with Telos Corporation (www.telos.com). He can be reached at dan.sherman@telos.com or on Twitter @0xjudd.



Authors: Merike Kaeo | Pages: 768 | Publisher: Cisco Press |

Designing Network Security is a book that will teach you how to secure your corporate network infrastructure. Starting with security fundamentals, you'll learn how to define a security policy for your enterprise and how to implement it, then finish with learning from examples of practical implementation concerning physical and network infrastructure.

About the author

Merike Kaeo is a consultant focusing primarily on security-related products and network design solutions. She has been in the networking industry more than 15 years.

She was employed by Cisco Systems for 7 years, where she worked primarily on technical issues relating to router performance, network routing protocols, network design, and network security.

Inside the book

The first part of this book is dedicated to security fundamentals. First, you'll learn some things about cryptography, and after a few words about authentication, authorization and key management, you are ready to tackle a chapter on security technologies and another one on how these technologies are applied to networks.

Before starting to design a security policy, you must understand what threats you are facing.

If you have been keeping abreast of the threat landscape, you can skip this part and go straight to a handy chapter which will tell you where to begin when deciding on a security policy (usually, with the existing security guidelines), impress upon you the importance of assessing your assets and the risks tied to them, and make you cherish the 5 main elements of a security architecture.

A corporate security policy must define physical and logical security controls and ensure data confidentiality and integrity - as well as the integrity of the entire system.

Defining policies and procedures for the staff, and developing and implementing security training for them is also something to take into consideration.

The most important part of the book is the third, where you learn how to secure your corporate infrastructure, Internet access, remote dial-in access and various kinds of networks (VPN, VoIP, wireless) by configuring routers, switches, firewalls and network access servers.

Of course, this being a Cisco book, the devices described are those manufactured by the company, but the same things apply to devices from other companies - most of them have very similar features. Lists of commands and samples of configuration processes are given, along with warnings about potentially tricky situations if you forget to do something.

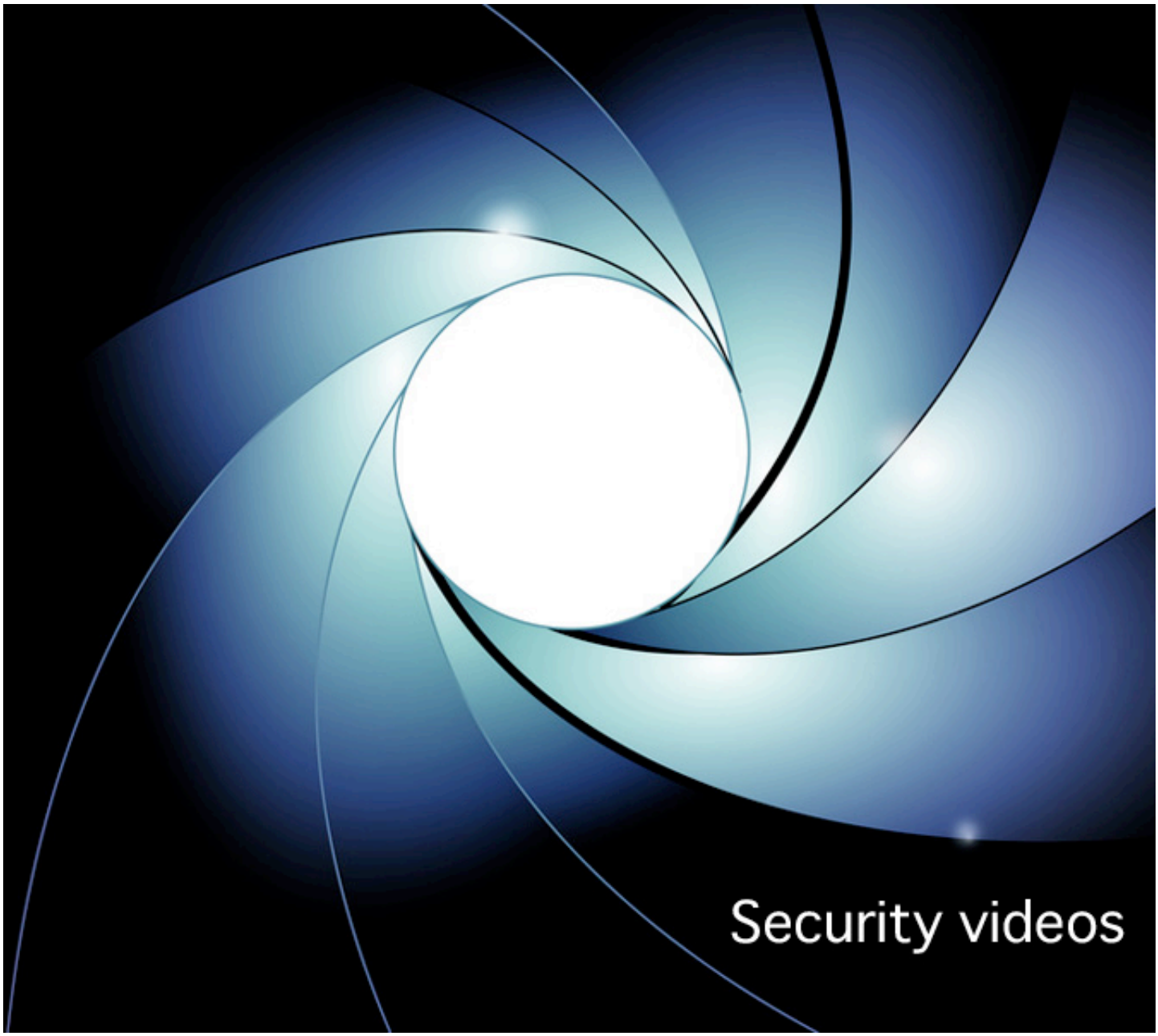
Each chapter is sprinkled with notes used to point out particular issues which a lot of people are not often clear on, and end with a short summary and review questions. A couple of appendixes about prevention of industrial espionage and mitigation of DDoS attacks are a welcome addition.

First published in 2004, this book has been revised and reviews of new security features and trends have been added.

Final thoughts

Designing Network Security is a formidable tome made for a specific purpose - to learn all the things you need to know when designing and implementing a corporate security policy. If you are looking for a light read that will sum up network security, this is not the book for you.

Zeljka Zorz is a News Editor for Help Net Security and (IN)SECURE Magazine.



BlindElephant: Open source web application fingerprinting engine
(www.net-security.org/article.php?id=1472)
Patrick Thomas, a vulnerability researcher at Qualys, discusses the open source web application fingerprinting engine BlindElephant.

Secure by design (www.net-security.org/article.php?id=1466)
David Grant, the Director of Security Solutions at IBM Rational, talks about how software is the invisible thread in a lot of innovations that enhance the quality of our lives.

Security B-Sides: The anti-conference (www.net-security.org/article.php?id=1473)
Security B-Sides co-founder Chris Nickerson talk about the concept and history behind the event, what's happening this year, as well as some future plans.

SSL Labs: Researching the technology that protects the Internet
(www.net-security.org/article.php?id=1476)
Ivan Ristic talks about SSL Labs - a non-commercial research effort and collection of documents and tools related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. Ivan is the director of engineering at Qualys and principal author of ModSecurity, the open source web application firewall.

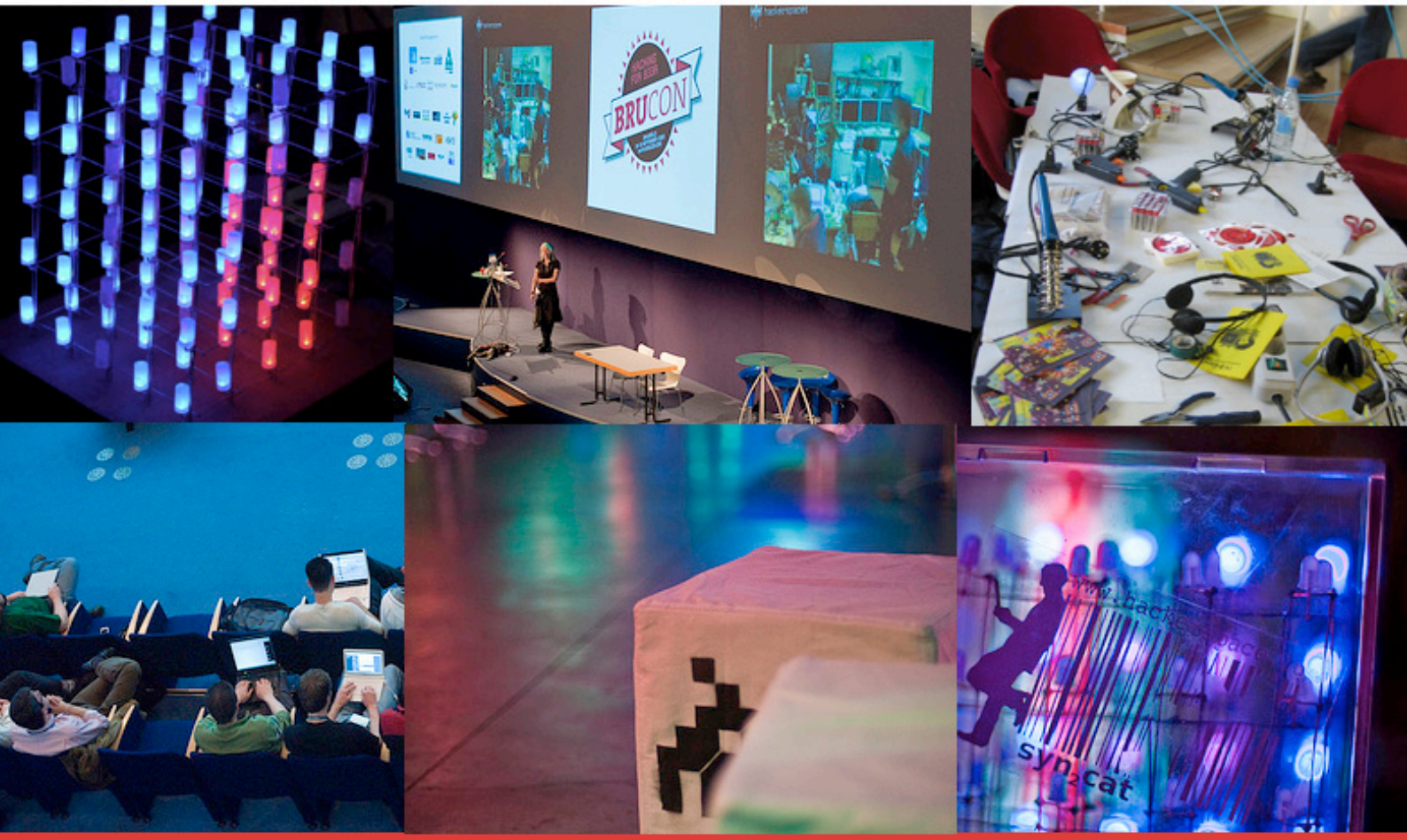
HACKING FOR B33R

BRUCON

SECURITY AND HACKER CONFERENCE

BRUSSELS, 24 & 25 September 2010

WWW.BRUCON.ORG



BruCON is an annual security and hacker conference providing two days of an interesting atmosphere for open discussions of critical infosec issues, privacy, information technology and its cultural/technical implications on society.

Organized in Brussels, BruCON offers a high quality line up of speakers, security challenges and interesting workshops.

More information available at http://www.brucon.org

Sponsors

Mediapartners

Want to become a partner or sponsor of a great event?
Contact us via http://www.brucon.org

Intelligent security: Countering sophisticated fraud

by Pat Carroll

The sophistication and increasingly widespread use of advanced fraudulent techniques such as Man-in-the-Middle and Man-in-the-Browser – two threats that traditional strong authentication techniques struggle to address – has forced banks and other organizations to re-think their approach to combating electronic fraud.

Customer authentication – No longer a sufficient means of protection

A number of high-profile fraudulent incidents in recent years have raised awareness of electronic fraud from the backroom to the boardroom, while also signaling a shift in electronic security strategy, in terms of both a holistic, multi-channel approach, and a re-evaluation of what 'customer authentication' actually provides.

The real impact of Man-in-the-Middle (MitM) and Man-in-the-Browser (MitB) attacks has been the realization that customer authentication, including strong multi-factor authentication, while being sufficient for certain transactions, cannot by itself prevent MitM and MitB attacks. Relying on a sophisticated combination of (usually client-side) injection attacks and impersonation of legitimate content or communication by an attacker, traditional end-point computer security measures can leave the end user vulnerable to fraud from attackers using the MitM and MitB approach. Therefore, these attacks have necessitated the requirement for 'Out-of-Band (OOB) Transaction Verification' in addition to strong authentication.

A typical MitB attack, such as the infamous 'Torpig', will involve the modification of web pages, modification of transaction content, or the insertion of additional transactions, all done in a completely covert fashion, invisible to both the user and the host application. So, while to an online banking customer it may appear that, for example, a certain sum of money has been transferred between bank accounts, they have actually been presented fake web pages, while the MitB attack has manipulated the transaction and diverted funds elsewhere.

However, the introduction of an OOB solution allows the end user to verify a transaction in real-time via (for example) a phone call that replays the transaction received by the bank so that the customer can confirm whether transaction integrity has been preserved.

Out-of-Band Transaction Verification verifies the integrity of the transaction itself, alerting the customer to any corruption of or tampering with the genuine transaction content, or even the creation of additional fraudulent transactions, thereby preventing the customer from unwittingly authorizing such transactions.

Automating the resolution process of Transaction Anomaly Detection (TAD)

Potentially fraudulent transactions, identified and intercepted by TAD or risk engines, require resolution of the potential anomaly. Typically, anomaly resolution is performed manually after the event. This involves an employee of a bank or call centre contacting customers by telephone in order to ascertain whether they have indeed performed a specific on-line transaction. This process is costly, unreliable insofar as actually making contact with the customer and insecure, as it involves a manual telephone call that could reveal security credentials to unknown third parties.

As electronic banking channels increasingly move to real-time transaction processing, the timeframe for dealing with anomalous transactions must also occur in real-time, i.e. before the transaction is committed. The introduction of Faster Payments in the UK in late 2007 is a case in point.

However, by automating the anomaly resolution process, and performing it in real-time, banks can overcome all of the present issues associated with manual follow-up, while also complying with real-time payments initiatives in a secure, timely and cost-effective manner. To securely automate this process requires transaction verification in addition to strong authentication, as it will increasingly be the transaction content that triggers the anomaly.

A combination of negative press, potential litigation and a perceived inability of institutions to offer a viable or convincing solution can bring to an escalation in the defection away from Internet banking.

Consumer confidence

Recent figures from the Financial Fraud Action (ukpayments.org.uk/files/fraud_the_facts_2010.pdf) show that fraud losses from online banking rose 132 percent between 2007 and 2008 to £52.5 million, and then rose a further 14 percent in 2009 to £59.7 million. The UK Cards Association (tinyurl.com/36gqlvv) attributes this rise to the more sophisticated malware attacks used by criminals targeting online banking customers. The high media profile of these security issues represents a significant opportunity for those banks to address the concerns of the public.

In addition to the direct fraud loss, banks can expect equal or even higher financial impact as a result of the associated administration costs. Furthermore, fraud issues in general may act as a significant barrier to potential customers, impacting on customer-base growth.

The sophisticated fraud now in evidence has the potential to further erode consumer confidence. A combination of negative press, potential litigation and a perceived inability of institutions to offer a viable or convincing solution can bring to an escalation in the defection away from Internet banking.

For those banks that seize the initiative in terms of offering truly secure Internet banking, there is also a clear opportunity, not just in reducing transactional costs within their existing customer base, but also in attracting new customers who are not offered similar secure services by their present financial institution.

These figures indicate a sizeable latent demand for secure Internet banking and a reason why security will be viewed as a significant differentiator between institutions.

Strong security for wider business enablement

Combining strong authentication with transaction verification provides the security necessary to ensure the integrity of a transaction and the identity of the user. This, in effect, creates a business-enabling technology that allows organizations to exploit the cost-effective Internet channel by allowing their customers to perform more self-service functions.

Transactions that traditionally have not been considered suitable for online processing, such as customer or account maintenance processes e.g. change of address forms or loan applications, that carry a high risk, can now be considered for migration to the Internet channel. Not only will the security afforded create a more consistent, accurate, and timely and secure process than the corresponding manual practices in place today, but it also empowers customers and creates potentially significant cost savings for the institution.

Intelligent security – Predict, prescribe, preempt

Using real-time, connected authentication models through telephony offers institutions intelligent options not available through static, disconnected devices. Indeed, a rules engine with dynamic rules (or triggers) can be applied to assess any transaction in real-time, forcing an authentication/verification when invoked.

Technologies such as transaction recording and biometric voice verification for non-repudiation, and operator breakout for potentially fraudulent transactions can all be combined to provide an exceedingly rigorous risk and compliance strategy, combining prediction of threat, prescription of countermeasure and preemption of attack.

Pat Carroll is the CEO of ValidSoft (www.validsoft.com). Prior to founding ValidSoft, he was Head of Electronic Trading Technology in Europe for Goldman Sachs International. In addition, he also performed the role of Co-Head of European Equities Technology and worked in an advisory capacity (technical due-diligence) with the Investment Banking Division of Goldman Sachs.

HELP NET SECURITY

WWW.NET-SECURITY.ORG

12 years of information security coverage