(IN)SECURE

OPEN. INFORMATIVE. TO THE POINT. Issue 13 - September 2007

INTERVIEW WITH NOKIA'S HEAD OF PRODUCT SECURITY

THE CASE FOR AUTOMATED LOG MANAGEMENT IN MEETING HIPAA COMPLIANCE

A MULTI LAYERED APPROACH TO PREVENT DATA LEAKAGE

SECURE
EASY TO USE
AFFORDABLE
my pw
www.mypw.com

OR
my pw

TABLE OF CONTENTS

Welcome to issue 13 of (IN)SECURE, a number we choose to consider as lucky! Lazy August and a very warm summer are behind us, and the time has come to get back to work and realize that the security issues you left behind when going on holiday are still here, probably getting worse.

Our collaboration with Addison-Wesley continues and we have another book giveaway where 5 lucky readers will get some free knowledge. The response for the previous giveaway was quite excellent and I'd like to thank everyone who sent in their comments about the magazine, you're helping us improve.

Keep the e-mails coming and if you're interested in contributing and getting read by a large number of security professionals and enthusiasts we're waiting for you to get in touch.

Mirko Zorz
Chief Editor

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: Mirko Zorz, Chief Editor - editor@insecuremag.com

Marketing: Berislav Kucan, Director of Marketing - marketing@insecuremag.com

Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor. For reprinting information please send an email to reprint@insecuremag.com or send a fax to 1-866-420-2598.

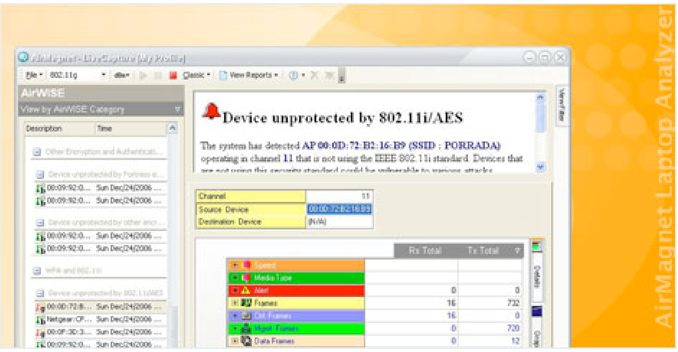
Corporate security news

Trend Micro goes the Software-as-a-Service way with SecureCloud

Trend Micro announced SecureCloud, their complete Software-as-a-Service Security platform offering its industry leading threat protection solutions for small, medium and enterprise businesses. The SecureCloud security platform has three dimensions that together create a complete Software-as-a-Service solution: security policy for all types of users, protection against threats across email and the Web that includes Web reputation, anti-malware and comprehensive content security and services that deliver security across all elements of the customer's infrastructure from gateway to desktop. (www.trendmicro.com)

World's first mobile WLAN analyzer for 802.11n networks

AirMagnet recently announced AirMagnet Laptop Analyzer 7.5, the industry's first mobile WLAN analyzer to natively decode and analyze 802.11n Wi-Fi networks. It provides instant visibility into all wireless channels, devices, conversations, speeds, interference issues and the RF spectrum, setting the standard for pre- and post-deployment management of 802.11n networks. The product will identify and classify 802.11n capable devices, identify higher data rates and channel modes, detect hundreds of security and performance threats, locate 802.11n rogue devices, provide troubleshooting tools and more. The release also adds support for the Windows Vista. (www.airmagnet.com)


AirMagnet Laptop Analyzer
File
802.11g
Classic
View Reports
AirWISE
View by AirWISE Category
Description
Time
Other Encryption and Authenticati...
Device unprotected by Fortress a...
Device unprotected by other encr...
WPA and 802.1X
Device unprotected by 802.11i/AES
Speed
Media Type
Alert
Frames
Ctrl. Frames
Mgmt. Frames
Data Frames

Device unprotected by 802.11i/AES

The system has detected AP 00:0D:72:B2:16:B9 (SSID : PORRADA) operating in channel 11 that is not using the IEEE 802.11i standard. Devices that

Channel	11
Source Device	00:0D:72:B2:16:B9
Destination Device	(N/A)

	Rx Total	Tx Total
Speed		
Media Type		
Alert	0	0
Frames	16	732
Ctrl. Frames	16	0
Mgmt. Frames	0	720
Data Frames	0	12

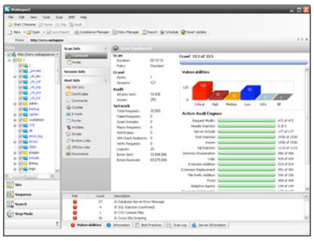
ESET Linux and FreeBSD security software betas

ESET Mail Security protects e-mail messages and e-mail gateway servers against known and unknown viruses, worms, Trojans, spyware, phishing, spam and other Internet threats.

Moreover, POP3, SMTP and IMAP protocols can be transparently scanned. ESET File Security provides antivirus protection for file servers and also offers user-friendly web administration interface. ESET Gateway Security is a new product for gateway servers, which offers transparent protection for HTTP and FTP. (www.eset.com/linuxbeta)

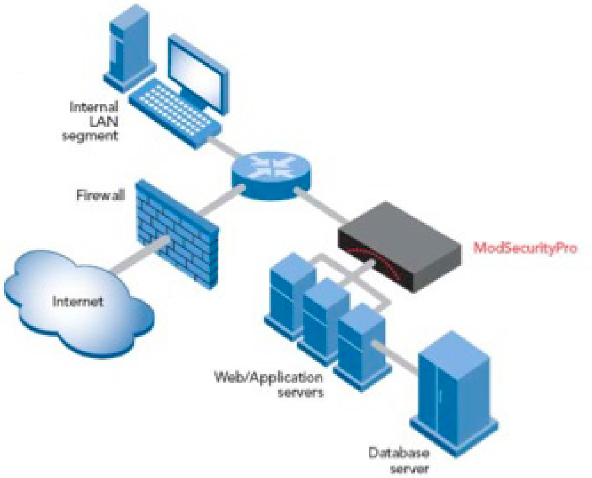
New application security software from SPI Dynamics

SPI Dynamics announced WebInspect 7.5, product re-architected to thoroughly analyze today's complex web applications built on emerging Web 2.0 technologies such as Ajax, SOAP, SOA and Flash.



The new architecture delivers faster scanning capabilities, broader assessment coverage, and the most accurate results of any web application scanner available. (www.spidynamics.com)

New Web application firewall appliance based on ModSecurity



Breach Security announced a new addition to its popular ModSecurity Pro web application firewall appliances product line with the launch of the ModSecurity Pro M1100. This new appliance offers immediate protection for production applications against targeted attacks with plug-and-play installation and enhanced rule sets.

The M1100 includes the mature, proven open source ModSecurity software, which is the most deployed web application firewall available today with more than 10,000 deployments worldwide. (www.breach.com)

New corporate antispyware solution with antivirus functions

Webroot Software announced the release of Webroot AntiSpyware Corporate Edition with AntiVirus.

In addition to compatibility with the Windows Vista operating system, key new features include Active Directory integration for simplified network deployment, Behavioral Genotype protection from Sophos which analyzes viral behavior to prevent it from executing, and the latest updates to Webroot's award-winning antispyware technology. (www.webroot.com)

Application control software and device management USB device combo

PatchLink is working with RedCannon Security to empower organizations with best-of-breed protection against the severe threats of data leakage and malware introduction via USB devices. A combination of PatchLink's Sanctuary policy-based device and application control software with RedCannon's KeyPoint Alchemy solution for device management creates a joint solution that includes identity management, user authentication and endpoint policy enforcement for the mobile workforce. (www.redcannon.com)

Early-warning system for Web 2.0 threats

Websense unveiled new technology that finds security attacks launched within Web 2.0 applications and delivers threat protection to customers within minutes. The increased popularity of these applications has also driven hackers to target users and businesses using these emerging tools. To combat this threat, Websense has deployed new systems called "HoneyJax" that emulate user behavior within Web 2.0 applications to uncover threats before they spread. Developed within Websense Security Labs and now part of the Websense ThreatSeeker technology, HoneyJax are the next evolution of "honey-based" systems designed to attract attackers and malicious code. (www.websense.com)

Oracle's new user authentication services for Linux

Oracle announced the preview release of Oracle Authentication Services for Operating Systems, a new offering within Oracle Identity Management. It is designed to make user management in operating systems more efficient, secure and centralized. Together with Oracle Internet Directory, a highly scalable LDAP directory that leverages the high availability and security features of the Oracle Database, Oracle provides a pre-integrated, easy-to-install and configure, centralized user authentication and storage solution for Linux and Unix. (www.oracle.com)

Secure USB 2.0 drives with hardware-authentication lock

Corsair launched the "Flash Padlock" family of affordable USB 2.0 drives, the safest way to secure your data while on the go. Priced starting at only $29.99 USD MSRP, Flash Padlock features "Auto-Locking," so the user doesn't need to remember to enable the protective feature—It will automatically lock and protect itself after removal from the computer. With its simple touch-pad security PIN entry system, Flash Padlock can be unlocked quickly and confidentially for use as a standard USB flash data drive. It is impervious to "brute force" hacks or keystroke loggers that would defeat a software secured USB flash drive. (www.corsair.com)

Interview with Janne Uusilehto, Head of Nokia Product Security

By Mirko Zorz

Janne is Head of Nokia Product Security, responsible for product security development at the world's number 1 mobile device manufacturer. He is a member of several Nokia internal security related management boards, and Nokia's main representative in the Trusted Computing Group and EICTA's Mobile Security Group. He is a frequent speaker at security conferences.

What is your background and how did it prepare you to face the challenges in your current position?

If I look back over my career, there is one common denominator and that is the Internet. I started my working life in software development for small and medium sized businesses, while using the majority of my free time surfing the Internet.

In the 90s I was working in the banking industry responsible for electronic banking related tools and software. This was the time when Internet sales, payment and banking systems really took off and this gave me great experience which I can rely on now as Nokia expands its focus from mobile devices to a range of Internet services.

What new trends and technologies do you find exciting?

I believe that the transition from simple voice centric phones to fully open Internet and open source software based personal devices with standardized platform features is fascinating. The mobile industry has learned a lot from the PC industry and right now we can see how those learnings will make a difference. More generally, the evolution to multimedia experiences and complete freedom of time and place are very very exciting.

What is your policy when it comes to establishing security rules for new products?

The main principles that we bear in mind when designing new products are high usability and putting maximum control in the hands of the device owner and user. The settings are made to meet the standard needs, and after this, the user can decide what level of protection he or she needs.

How does security integrate into the product manufacturing life-cycle of Nokia business phones? How important is security to Nokia's overall product strategy?

I used to say that "security is equally important as any business enabler, no more, no less". Security is a vital part of devices targeted to business segments, but has a significant role in other devices and segments as well. Differences become evident if we look at security more closely. Platform and system security must be well defined and accurately targeted in both. The clear difference is in the area of security services for mobile devices, such as terminal management and VPN systems. One key area where we have invested heavily is mobile device management, technology which allows IT organizations remotely manage their IT security policies on their Nokia business devices based on their individual and organizational requirements.

Security must be part of the design process, right from the start of platform development. In order to be effective enough, security can not be added afterwards, when the device design is completed.

Most of your high-end devices run Symbian but Linux is coming into the picture. In your opinion, which platform is more likely to stand the test of security over time?

My view is that there are no major differences between these platforms when it comes to security. Most of the protection is based on architectural design and applications used on top of the platform. Both are designed for demanding security environments. And both have their target customers and user groups. My responsibility is to make sure that Nokia has an innovative and competent product security development organization for any platform that we use. We are exploring the use of Linux in our non-cellular device category through the Nokia N800 and 770 Internet Tablets.

What security strategy does Nokia have in order to maintain a firm grip on the variety of evolving threats targeting mobile devices?

Our strategy for security developments in Nokia products and platforms is based on detailed analysis of the demand for different features and services. When either the user or business case indicates that more security features and/or services are needed, those are made part of the default set. Platform security can also be adjusted based on needs identified in the analysis. Having an open platform means that the user of the device can increase the level of security as needed.

What security challenges does Nokia's product portfolio face in the next 5 years?

What will happen in the future is hard to guess and I don’t have a crystal ball! Our work is based on a straightforward strategy that consists of thorough threat analysis, product by product, platform by platform.

From experience, although technologies are evolving, the principle types of threat remain the same, though the details may vary. A structured approach such as ours allows us to plan and respond effectively. As the mobile environment evolves, we are seeing that most of the threats today are familiar from the Internet and computer environments, attacks are just targeted to new implementations and new protocols.

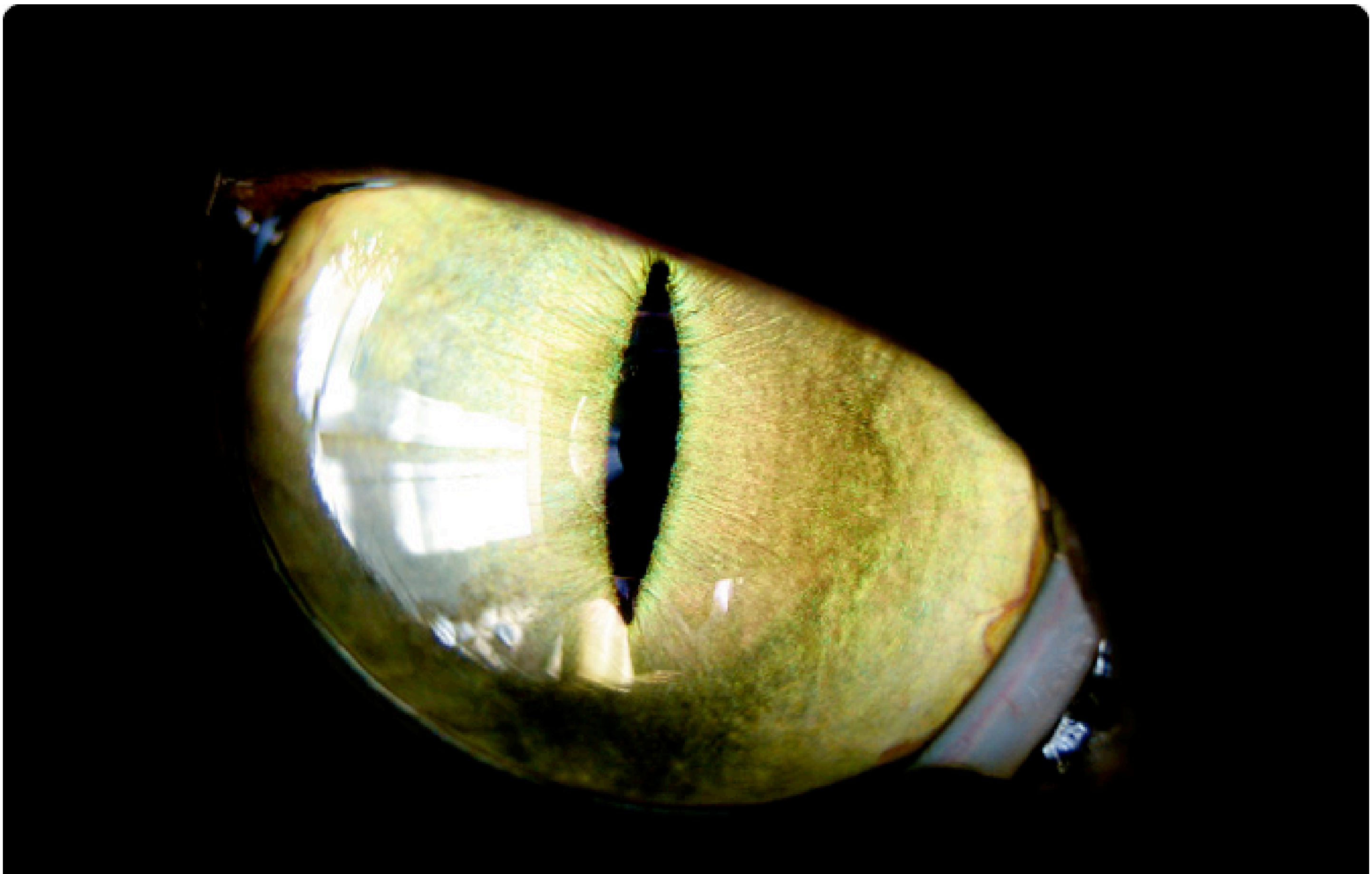
To prepare for this challenge, we are designing our devices today to deliver a robust set of security capabilities and also to enable our users to protect themselves without compromising the mobile experience that they love

What can enterprise customers expect from Nokia in 2008 when it comes to security?

Nokia business customers will be able roll out new and exciting mobile applications to securely liberate their workforce from their cubicles and enable cost savings with technologies such as mobile email and VoIP from Nokia and its partners and standardize on Nokia security platforms.

Let's finish with an easy question. I'm sure many of our readers are wondering - what mobile phone/smartphone do you use? Why?

Hmm.. this is not an entirely fair question as I like different types of gadgets very much. But 95% of the time I'm using my Nokia E61i, at times a Nokia N95. For Web browsing and Internet communications, I sometimes use a Nokia N800 Internet Tablet.



Social engineering social networking services: a LinkedIn example

By Nitesh Dhanjani

The term Identity Theft is usually assumed to be related to a malicious entity abusing someone's credit information to commit financial fraud. This continues to be a big problem, but I'd like to extend the problem of identity theft in the social-networking aspects of so-called Web 2.0 applications.

I feel this is an important topic of discussion because, unlike technical vulnerabilities that can be remediated with a software patch, the problem at hand is a design issue that poses significant risks to society's ability to securely leverage the usefulness of social networking.

Before I go any further, I'd like to make it extremely clear that I am a big advocate of the emerging online social networking applications. I feel the new paradigms of sharing offered by some of the new services today have changed the way we interact for the better and I am personally delighted to be a part of this culture shift. I also feel that information security should act as an enabler by helping understand the security consequences in design and implementation in addition to a discussion of risk and remediation. In no way, shape, or form is the purpose of this post to suggest that the concept of social networking is 'bad' or 'evil'. The purpose of this article is solely to (informally) discuss concerns in order to work towards a more secure way of dealing with these new systems.

I'd also like to deal with the most common knee-jerk reaction to the topic: *people are the easiest target, so there is no point in even trying*. It is true that people are the easiest attack vector, but I don't think it helps the situation any when we start out thinking about the problem in this way. People are indeed an easy target, but it is the people's self-interest we are trying to protect in the first place. The job of information security is to make it harder for people to do wrong things.

Getting back on topic: the fundamental problem with online social networking services is that they offer no way of authenticating a given identity. This may not appear to be a big issue at the moment, but I feel this will start (perhaps already has to a certain extent) to become a security nightmare and a social engineer's dream come true. Our privacy, reputation, and identities are at stake.

The concept of the potential abuse of online social networking services is not new. I am not the first to talk about this topic. There has been a lot of discussion on this issue amongst the security community since the past few years. What I'd like to do here is enumerate a few concerns that I have been pondering over and to try and spread a little more awareness.

The fundamental problem with online social networking services is that they offer no way of authenticating a given identity.

I'd like to select LinkedIn (www.linkedin.com), the popular social networking service, to illustrate my concerns. Other social networking sites (examples: Digg, del.icio.us, Facebook, Flickr, Myspace, Orkut, Twitter) are also similarly susceptible, but I'd like to stick to LinkedIn for the sake of brevity.

Intellectual Property

Assume that you are in the consulting business. In this situation, your client points of contacts are extremely important to you, and you probably wouldn't want to share your address-book with your competitors. In this situation, your address book is your intellectual property that you want to share in a way with people such that it is mutually beneficial, and this is indeed what LinkedIn is all about. Unfortunately, this is hard to do in a secure way because LinkedIn does not offer a way to authenticate identities. At the most, LinkedIn relies upon email as the identity token - this is hardly a reliable (or even feasible) method of identification: people have multiple email addresses, some use their work email address, and some prefer to use their yahoo or gmail accounts. With the prior scenario in mind, an easy way to grab hold of a competitor's address book on LinkedIn is to get them to 'connect' to you:

a. Think of an individual the target LinkedIn member may know.
b. Create an email address with the name of this individual using
firstname.lastname@yahoo.com or
firstname.lastname@gmail.com. You can go as far as creating a similar looking domain name of the company the individual may work at (@applee.com, @app1e.com, etc).
c. Create a profile on LinkedIn with the name and e-mail address of the individual.
d. Send an invitation to the target using the new LinkedIn account, and wait for the target to accept.
e. BONUS: Other people the target is connected to will notice that he or she has added a new friend (the individual you picked). Should the individual happen to be a mutual friend of these people, they will likely attempt to connect to your new LinkedIn profile, offering you even more details into the network of the target.

This example is specific to LinkedIn, but the idea applies to other services as well. This problem is likely to grow in severity as society becomes reliant on online social networking without a secure way of identifying whom it is you are networking with.

Privacy

In order to be a part of a mutually beneficial social system, people have to share information with each other for the system to work. In this situation, the issue of keeping critical information a secret is the most obvious one. Given the sheer excitement and instant benefit of the social applications today, it is very difficult to maintain self-discipline on what sort of information you are about to give away.

Another issue I'm interested in at the moment is the potential of remote behavior analysis. For example, I've noticed that people who start looking for new jobs have a tendency to add a lot of new contacts on LinkedIn in a short period of time. This may be an issue for someone who doesn't want his or her current employer to know. I feel that we are likely to see more formal methods of such types of behavior analysis in the near future. Perhaps this may sound a tad far-fetched at the moment, but I can easily imagine the feasibility of a system that would spider for information about you to make a prediction of your current thought processes: What types of bookmarks are you tagging (del.icio.us)? What types of photographs are you tagging (Flickr)? What are you doing these days (Twitter) ? What are your friends saying to you and about you (Facebook, Orkut, MySpace)? You get the idea.

Reputation

As the popularity of search engines has increased, people have increasingly become aware that it is hard to erase personal footprints from the Internet. As with the privacy topic, it is hard to maintain this sort of self-discipline on what you say or do amongst the social networking paradigm for the sheer and instant gratification of the perceived benefits - the risk of losing reputation is only realized later on. I am not immediately interested in this problem because I feel this is the most obvious side effect of the system in general. What I am more concerned about is the problem of unfair perception. For example, we all like to share funny YouTube videos, but as researchers to formalize the process of gathering data about an individual in this way, the result can lead some amount of unfair analysis. Perhaps one example of this idea is the brilliant wikiscanner (”list anonymous Wikipedia edits from interesting organizations”). It can be argued that wikiscanner can be used to accurately identify patterns that indicate an alleged conspiracy by a given company to edit or vandalize wikipedia for their benefit. But in all fairness, the situation is most likely to be a group of mischievous employees at the company.

Another problem at hand is that of someone assuming your identity whilst tarnishing your reputation. Even though there is no concept of a reliable identity mechanism in social networking applications today, people have a tendency to immediately believe what they read. For example, consider a scenario where someone sets up a profile on LinkedIn with your name to contain false information that is unflattering. This is likely to become a problem should a potential employer search for “your” profile.

Reconnaissance

One of the first things a malicious attacker will do before attacking the interests of a given organization or individual is to perform reconnaissance. Any publicly available information is a freebie and an aid to the attacker. The target in question can be an individual's or an organization's computer network and data. I invite you to check out Maltego (www.paterva.com/web/Maltego/index.html), a fantastic and free tool that demonstrates how easy it is to obtain wealth of information about a given person or organization.

So what are we to do? I think the first logical step is to spread awareness and comprehend the side-effects of sharing information. We are sharing and communicating ideas like never before, and we need to comprehend the applicable risk-benefit ratios. From a technical perspective, something like OpenID seems to be a step in the right direction but I think we still need an agreeable solution to link an individual with a given token based identity.

From a philosophical perspective, maybe the cost of the popularity of an individual to token identification system will negatively impact the usefulness of the Internet culture that thrives on a sense of anonymity. Perhaps the emergence of these social network services will impact cultures around the world to open up and be more accepting, thus eliminating some of the concerns outlined above.

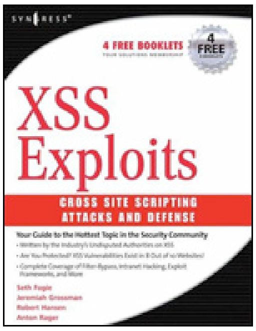
Nitesh Dhanjani is the author of "Network Security Tools: Writing, Hacking, and Modifying Security Tools" and "HackNotes: Linux and Unix Security". He is currently the Senior Director of Application Security Engineering at a large corporation in the US. Prior to this, Nitesh was a Manager at the Advanced Security Labs at Ernst & Young LLP. Prior to Ernst & Young, Nitesh consulted for Foundstone where he contributed to and taught Foundstone's "Ultimate Hacking: Expert" and "Ultimate Hacking" security courses. Nitesh has performed hundreds of security assessments, including Attack & Penetration reviews, source code reviews, and security architecture reviews for many of the Fortune 500 companies.

Latest additions to our bookshelf

XSS Exploits

By Seth Fogie, Jeremiah Grossman, Robert Hansen, Anton Rager

Syngress, ISBN: 1597491543

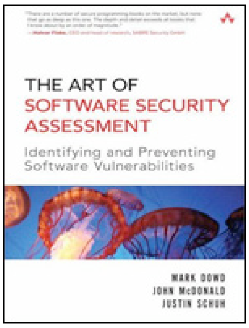


XSS Exploits starts by defining the terms and laying out the ground work. It assumes that the reader is familiar with basic web programming and JavaScript. First it discusses the concepts, methodology, and technology that makes XSS a valid concern. It then moves into the various types of XSS attacks, how they are implemented, used, and abused. After XSS is thoroughly explored, the next part provides examples of XSS malware and demonstrates real cases where XSS is a dangerous risk that exposes internet users to remote access, sensitive data theft, and monetary losses. Finally, the book closes by examining the ways developers can avoid XSS vulnerabilities in their web applications, and how users can avoid becoming a victim.

The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities

By Mark Dowd, John McDonald, Justin Schuh

Addison-Wesley Professional, ISBN: 0321444426

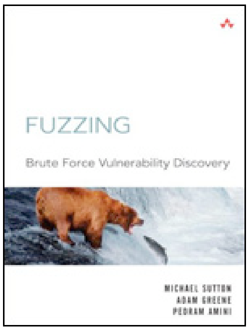


The Art of Software Security Assessment covers the full spectrum of software vulnerabilities in both UNIX/Linux and Windows environments. It demonstrates how to audit security in applications of all sizes and functions, including network and Web software. Moreover, it teaches using extensive examples of real code drawn from past flaws in many of the industry's highest-profile applications. Drawing on their extraordinary experience, authors introduce a start-to-finish methodology for “ripping apart” applications to reveal even the most subtle and well-hidden security flaws.

Fuzzing: Brute Force Vulnerability Discovery

By Michael Sutton, Adam Greene, Pedram Amini

Addison-Wesley Professional, ISBN: 0321446119

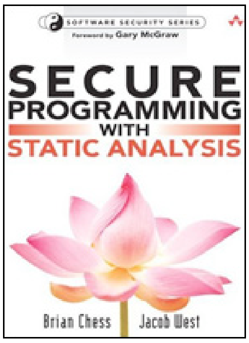


Fuzzing is the first and only book to cover fuzzing from start to finish, bringing disciplined best practices to a technique that has traditionally been implemented informally. The authors begin by reviewing how fuzzing works and outlining its crucial advantages over other security testing methods. Next, they introduce state-of-the-art fuzzing techniques for finding vulnerabilities in network protocols, file formats, and web applications; demonstrate the use of automated fuzzing tools; and present several insightful case histories showing fuzzing at work.

Secure Programming with Static Analysis

By Brian Chess, Jacob West

Addison-Wesley Professional, ISBN: 0321424778



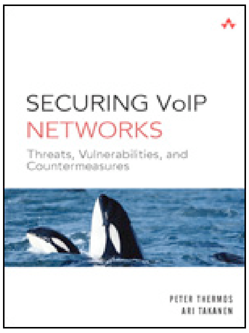
Static analysis experts Brian Chess and Jacob West look at the most common types of security defects that occur today. They illustrate main points using Java and C code examples taken from real-world security incidents, showing how coding errors are exploited, how they could have been prevented, and how static analysis can rapidly uncover similar mistakes.

This book is aimed towards everyone concerned with building more secure software: developers, security engineers, analysts, and testers.

Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures

By Peter Thermos and Ari Takanen

Addison-Wesley Professional, ISBN: 0321437349



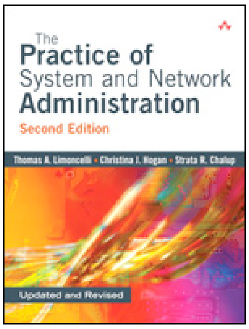
Written by two industry veterans, this book delivers quality information regarding threats, vulnerabilities as well as the very important countermeasures. This title is aimed at an audience of security professionals that like to venture into technical material. The authors manage to get the most important message through - when deploying VoIP networks, you need to tailor security practices based on your needs from the very beginning.

Read a complete review at: www.net-security.org/review.php?id=158

The Practice of System and Network Administration (2nd Edition)

By Thomas Limoncelli, Christina Hogan and Strata Chalup

Addison-Wesley Professional, ISBN: 0321492668



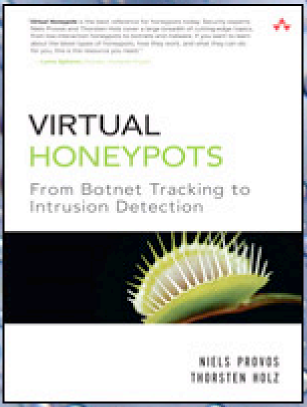
Despite being thick as a phone book, you'll see that this book is very clearly organized and can serve not just as a learning tool but also as an effective reference guide for seasoned system and network administrators. When it comes to work that system administrators are doing the most, this book deals with topics such as data integrity, network devices, debugging, customer care, server upgrades, service monitoring, and everything else you may need.

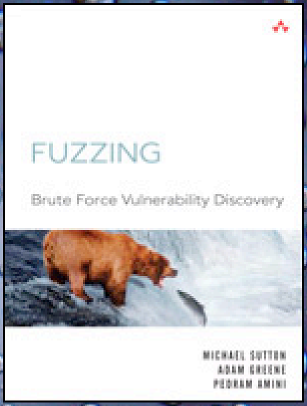
Read a complete review at: www.net-security.org/review.php?id=159

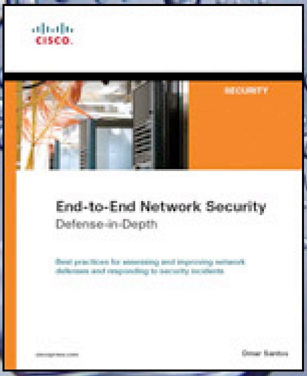
Want some knowledge?
Enter our book contest!

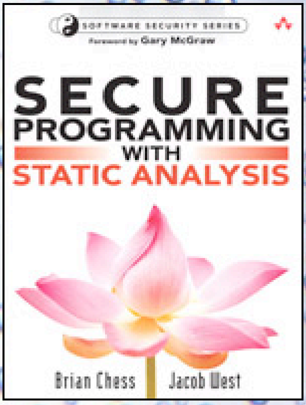
ADDISON-WESLEY

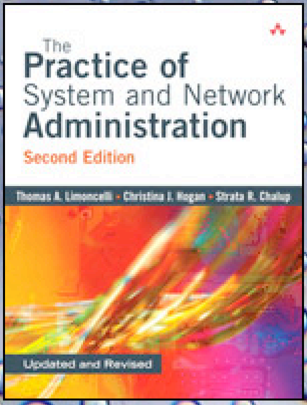
We are giving away a copy of the following titles:











What do you have to do?

Go to www.insecuremag.com/contest to enter.

The contest ends October 19th 2007.

The case for automated log management in meeting HIPAA compliance

By A.N. Ananth

The Health Insurance Portability Accountability Act, better known as HIPAA, was passed in 1996 by the US Department of Health and Human Standards (HHS) to ensure the privacy and security of confidential patient health information.

The Act mandates that all Covered Entities (CEs) must implement 'reasonable and appropriate' procedures for securing patient health information from security breaches, impermissible uses and/or disclosures, with severe penalties mandated to punish non-compliance.

In March, Atlanta's Piedmont Hospital became the first institution in the country to be audited for compliance with the security rules of HIPAA. The audit was conducted by the office of the inspector general at HHS and is being seen by some in the healthcare industry as a precursor to similar audits to come at other institutions.

A number of HIPAA requirements are focused towards the integrity of electronic protected health information (ePHI) – any personally identifiable health information that is handled electronically, including:

- Controlling access to ePHI
- Monitoring and auditing access to ePHI
- Diagnosing potential security problems
- Retaining records of access for a set period of time
- Demonstrating to independent reviewers the processes that fulfill the requirements above.

In the Piedmont case, it was reported that HHS asked for this type of information to be provided within 10 days. In the absence of automated log management systems that record and maintain this information, producing it became a very challenging, manual effort.

Log management, specifically, can be directly applied to the following 7 HIPAA recommendations and requirements:

	Requirement	Details
I	**Review of Information System Activity § 164.308(1) (ii) (D)**	Implementation of procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident reports.
II	**Protection from Malicious Software § 164.308(a)(5)(ii)(B)**	Calls for procedures for guarding against, detecting and reporting on malicious software.
III	**Log-in Monitoring § 164.308(a)(5)(ii)(C)**	Monitoring log-in attempts and reporting discrepancies.
IV	**Security Incident Procedures §164.308(a)(6)(ii)**	Implementation of methods to identify and respond to suspected or known security incidents; mitigate to the extent practicable.
V	**Audit Controls § 164.312(b)**	Implementation of hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
VI	**Integrity & Authentication of ePHI § 164.312(c)(1) and (2)**	Electronic measures to corroborate that ePHI has not been altered or destroyed in an unauthorized or improper manner.
VII	**Person or Entry Authentication § 164.312(d)**	Procedures to verify that a person or entity seeking access to ePHI is the claimed.

Table 1.

In order to successfully meet the above requirements, HIPAA specifically calls out event logs as an important vehicle to meet compliance and requires CEs to collect, analyze, preserve, alert and report on system and application security event logs generated by all relevant systems.

In fact, many other regulatory mandates and best-practice processes also recommend regularly reviewing log data in order to achieve complete network transparency and diagnose potential security problems. Apart from helping with compliance, this also benefits healthcare organizations by providing patients with the confidence that their most sensitive data is secure and protected from misuse.

Can this be achieved without an automated log management solution in place? The answer to that is ‘possibly’, but especially at the larger CEs, at a considerable risk of information breach and audit failure.

In a 2006 survey on ‘the state of HIPAA privacy and security compliance’ conducted by the American Health Information Management Association, only 39% of hospitals and health systems reported full privacy compliance. Why are companies failing to comply? Importantly enough, the survey found that 55% of respondents identified resources as their most significant barrier to complete privacy compliance – Certainly, most healthcare organizations do not have dedicated security operation centers or staff to routinely and consistently audit event log data for successful compliance.

The challenge lies in the variety of data sources that exist across a network, different log formats and the massive volume of log data generated daily by a healthcare organization. Event log management and analysis for healthcare companies becomes all the more time-consuming and costly given the confidential nature of much of the information retained on their systems, multi-user workstations and the breadth and size of their networks.

These challenges tax the limit of most available resources, resulting in inefficiencies and breaches.

Why manual processes don't work

1. Collection and review

Database systems, critical applications, devices and multiple operating systems record a considerable amount of security data into local logs. At a bare minimum these logs need to be collected and archived in a central location for regular review in order to meet compliance.

Given that log generation can run into the hundreds of thousands in number, and continuously grow, it is next to impossible to rapidly collect them as they are generated.

These logs contain valuable information that, if accessible can detect potential security issues before they impact patients. However, it is difficult, not to mention inefficient, to view logs one at a time and make sense of them. Message formats vary widely and system-specific expertise is required to garner any sort of intelligence from the mountain of data. Furthermore, because tens of thousands of different event IDs and types exist, no one expert can have complete knowledge.

2. Storage

In order to facilitate review, log data needs to be stored securely for on-demand retrieval and historical analysis. Normally, a single Windows server can generate over 100,000 events every day without using the auditing feature.

With the audit feature in operation, Windows servers, like many UNIX systems, SNMP devices and firewalls, can produce over one million events per day. It is not unusual for even a small organization to generate well over 20 million events every day. This information needs to be securely archived for IT controls and compliance.

Although HIPAA does not specifically mandate that log data be stored for multiple years, industry best practices recommend a data retention policy of at least 6-12 months, in order to accommodate long-term investigation in case of a breach, as well as to assist with auditor interpretations.

One hundred Windows servers with an average number of 100,000 events each, means a total of 10 million events per day – and that is without auditing! If these events are kept for 90 days, it is necessary to manage and store 900 million events. Retained for 1 year, the archive would contain over 3.5 billion separate event records. This can translate into a significant storage burden, keeping in mind that one million events can take up to 5GB of space in a traditional database.

3. Analysis

Many of the conditions that indicate issues can only be detected when events are correlated or associated with events happening on other systems and devices. If caught in time, these signs can alert personnel to take the necessary actions before security is compromised. Moreover, this analysis needs to be done in real-time for immediate insight into unusual and suspicious user/network activity – a task that is impossible to do manually, unless of course, a company has an army of IT experts at its disposal 24/7.

4. Alerting

In order to quickly respond to suspected or ongoing security incidents, real-time alerting is critical. Without an automated solution in place, a user would have to manually access all systems one-by one, repeatedly to attend to any issues discovered.

5. Reporting

Another challenge when collecting thousands of logs is to organize them in a way that is reflective of the regulation. Although HIPAA specifically asks for access reports and security incident reports, many times it is not possible to understand in advance what an auditor might require. It might very well be that huge volumes of information is requested or very specific information pertaining to certain servers, time periods, users or events is asked for as proof of adherence.

Searching through log data in response to auditor questions can overwhelm even the most prepared organization if they do not have the appropriate technology in place.

Choosing the right solution for your HIPAA requirements

Look for an extensible collection engine, and a centralized console

Organizations, today, support a number of devices including firewalls, applications, databases, multiple operating systems etc. For a log management solution to be useful it must not only be able to collect event logs generated by a variety of disparate sources, but should also be able to capture log data from any custom application or system dealing with ePHI, and have the ability to quickly provide support for new devices. This collected data should be made available on an intuitive interface that centralizes reporting and analysis functions for rapid review across massive log volumes.
Applies to Requirements: I, II (See table 1 for mapping requirements).

Electronic Sign-off for closed loop operations

An automated log management solution must include support for closed loop operations where log collection, archiving, reporting are all supported. However, the matter does not end there. The solution must also support the workflow to permit IT staff to review automatically generated reports and sign-off on them in a tamper resistant manner. Auditors must be able to review the sign-off and associated comments easily, to establish adherence to review processes. Secure remote access for this feature will minimize operation costs and is desirable.
Applies to Requirement I.

Insure secure storage

Look for a solution that offers compressed secure tamper-proof storage that does not require costly database licenses or administrators. The solution chosen should also be able to store data in its entirety for a complete audit trail that describes the entire history of an event. This is essential for examining detailed historical activity of access to or modification of critical data.
Applies to Requirements: I, IV, V, VI.

The importance of real-time correlation and alerting

It is not enough for a solution to collect logs – a robust log management product should enable powerful real-time monitoring and rules-based alerting on the event stream. Rules can watch for seemingly minor unrelated events occurring on multiple systems across time that together represent clear indications of an impending security breach. For instance, multiple failed logins across all systems with a single remote IP address, or multiple unsuccessful login attempts to different accounts on a single system, are signs of a hack attempt. With real-time alerting, IT and security staff can be notified immediately when a suspicious activity is discovered, for quick remediation, before confidential patient information is impacted.
Applies to Requirements: I, II, III, V.

Integrated reporting is a must

Choose a solution that come integrated with pre-defined report templates typically required by regulatory mandates and standards. Ensure that custom reporting is provided for quickly responding to auditor queries of information, demonstrating a log review process and adherence to multiple requirements
Applies to Requirements: All.

Ask for change management capabilities

Look for a log management solution that delivers change and configuration management, key components for regulatory compliance and security management. These capabilities automate regular scanning of registry hives and configuration settings, which are then compared with initial assessments of the IT environment to reveal any critical changes such as prohibited and infected files and applications.
Applies to Requirement II.

Insist on Role-Based Access

Because log data contains sensitive information, especially in the case of healthcare organizations, access must be limited to authorized persons to minimize misuse. A log management solution must be able to restrict access to data according to corporate policies, assigned roles and privileges.
Applies to Requirements: VII.

Conclusion

The right log management solution, used in conjunction with internal procedures and policies, provides CEs with the capability to have a strong, yet cost effective compliance strategy in place, and to easily demonstrate adherence to external auditors. Managing log data manually, although possible, is an extremely labor intensive activity that not only puts an immense amount of stress on existing resources, but has the ability to detract from other processes and put huge holes in IT budgets. Not to mention, manual processes are subject to human inefficiencies which can translate to thousands of dollars in liability for non-compliance, remediation and other related expenses.

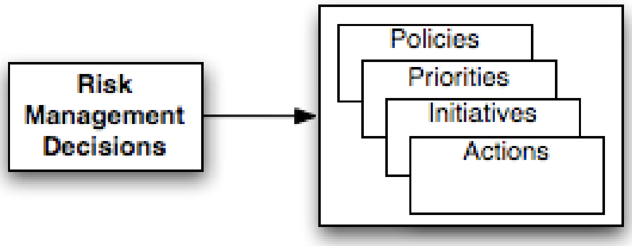
A. N. Ananth is the co-founder and CEO of Prism Microsystems, Inc. A leading expert in IT compliance with over 20 years experience in IT-control and operations, he has consulted for many companies on their compliance strategy, audit policy and automated reporting processes. Ananth was one of the original architects of the EventTracker product offering, Prism's enterprise log management solution, and remains active in strategic product direction at Prism.

Risk decision making: whose call is it?

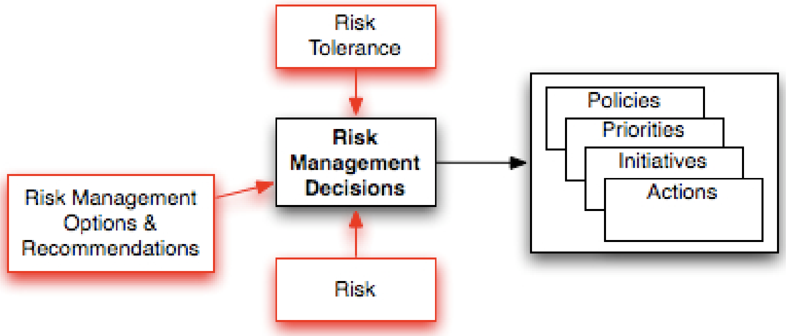
By Jack Jones

I still occasionally run into a debate with colleagues over whether security should be making the major information risk decisions for an organization, or whether it's business management's responsibility. Rather than just spew my opinion, let me try to build an illustration of how I view the problem.

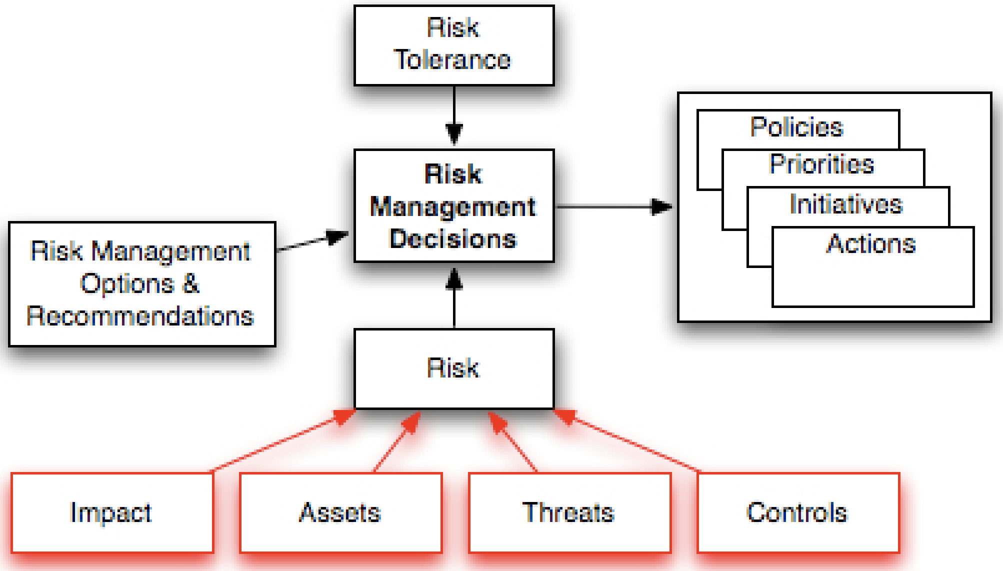
1. Risk decisions are the things that drive policies, priorities, initiatives, and actions (this falls under the category of "duh").



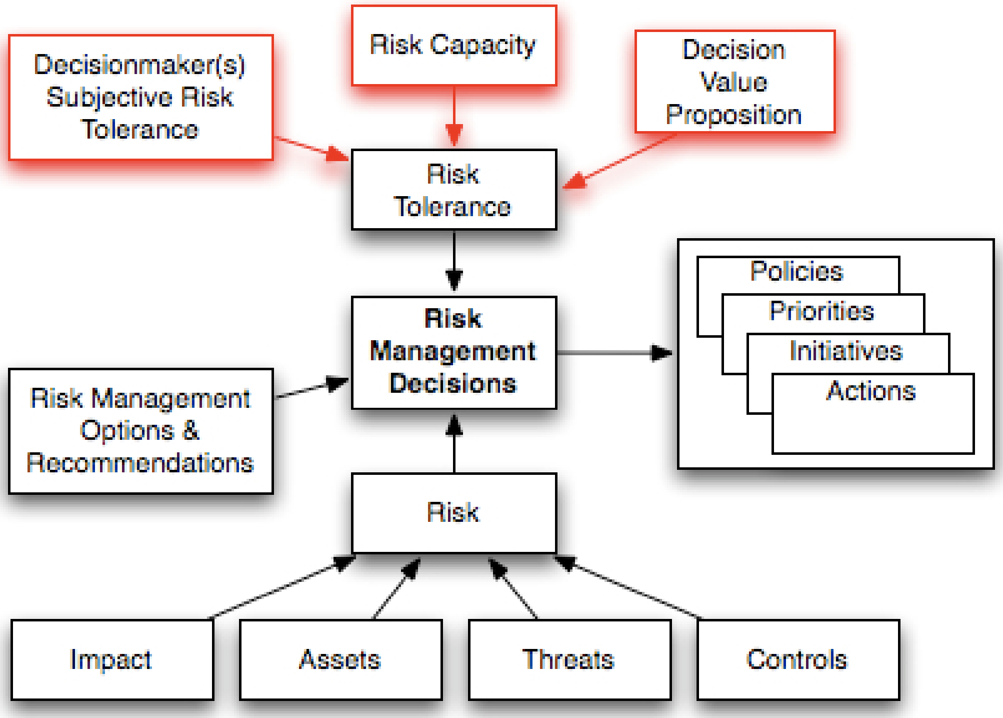
2. Well-informed risk decisions are dependent upon knowing the risk associated with the decisions, as well as the best risk management options. Risk tolerance also is an inevitable factor (we'll discuss the question of whose risk tolerance further on).


Risk Tolerance
Risk Management Decisions
Risk Management Options & Recommendations
Risk
Policies
Priorities
Initiatives
Actions

3. Understanding risk, of course, requires that we understand the factors that drive impact (stake-holders, laws, contracts, competitive landscape, etc.), the assets associated with impact, threats against those assets, and controls that are in place to manage risk. Absent any of these inputs, our understanding of risk can be seriously deficient and the resulting decisions flawed.



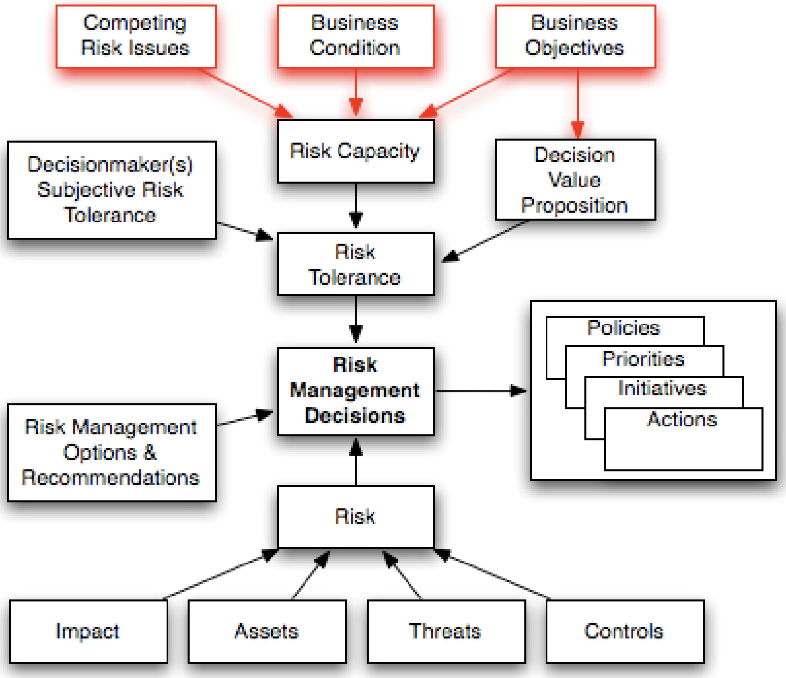
4. So far – no surprises. At this point, however, things begin to get a bit more interesting… Specifically, risk tolerance is derived from three inputs: risk capacity, the decision's value proposition (the potential upside associated with the risk scenario), and the decision-maker's subjective risk tolerance (more on this further on).


Decisionmaker(s) Subjective Risk Tolerance
Risk Capacity
Decision Value Proposition
Risk Tolerance
Risk Management Decisions
Policies
Priorities
Initiatives
Actions
Risk Management Options & Recommendations
Risk
Impact
Assets
Threats
Controls

5. Risk capacity also has three inputs; the organization's current condition relative to its objectives, as well as the portfolio of competing risk issues. It's important to recognize, too, that these factors will often vary across the different types of loss (e.g., productivity, competitive advantage, resources, reputation, etc.). For example, an organization that has a significant stockpile of resources will have more capacity for resource loss than will an organization that operates on a shoestring. Likewise, an organization that is trying to build market share will have less capacity for reputation damage than will one that already leads

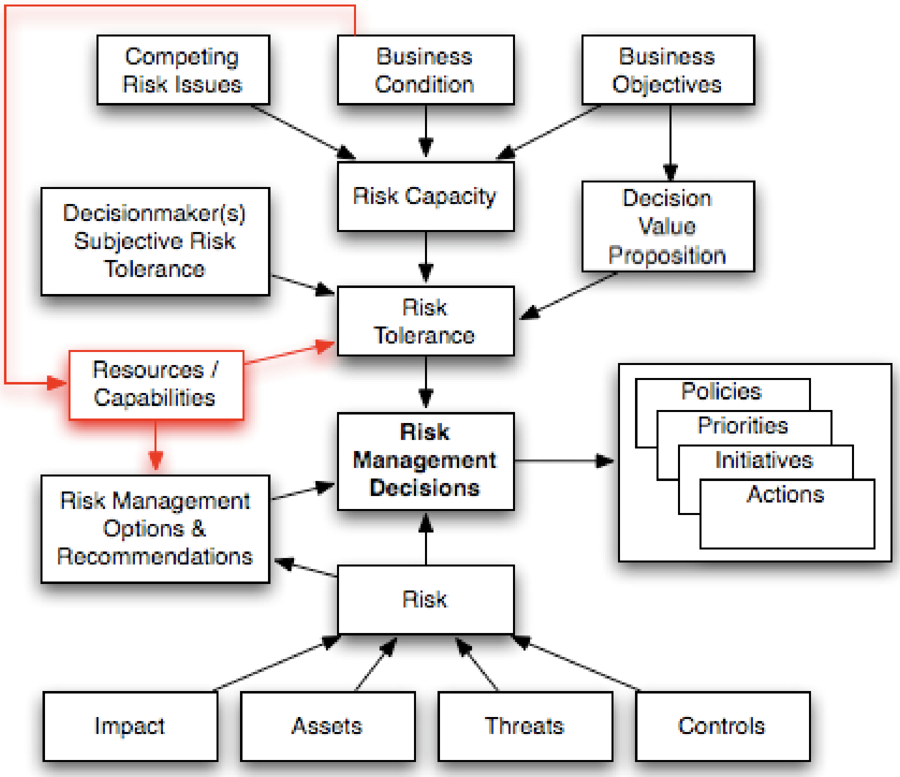
the competition and/or that has a very loyal customer base.

The point is, tolerances will vary not only between organizations but also between types of loss within an organization.

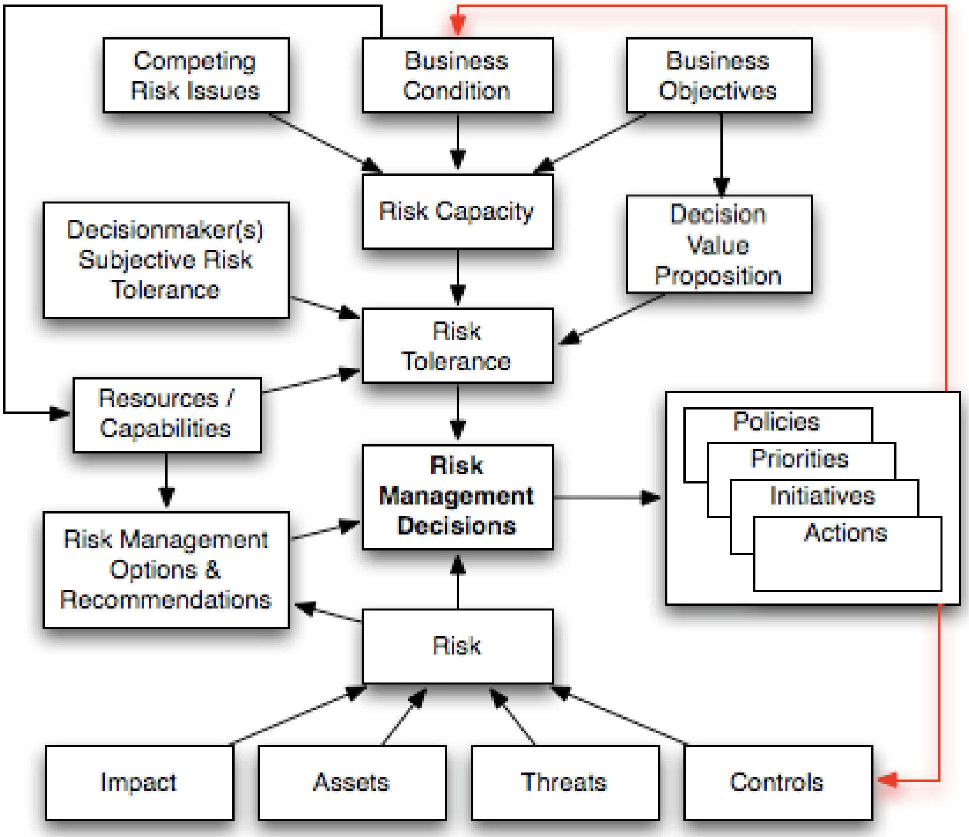


With regard to competing risk issues, it's important to keep in mind that information-related risk is only one of many risk domains management has to deal with (e.g., market, insurance, investment, etc.). Combine this with complex organizational conditions and objectives, as well as limited resources, and it becomes clear how important (and difficult) it is to strike the right balance in applying risk management resources.

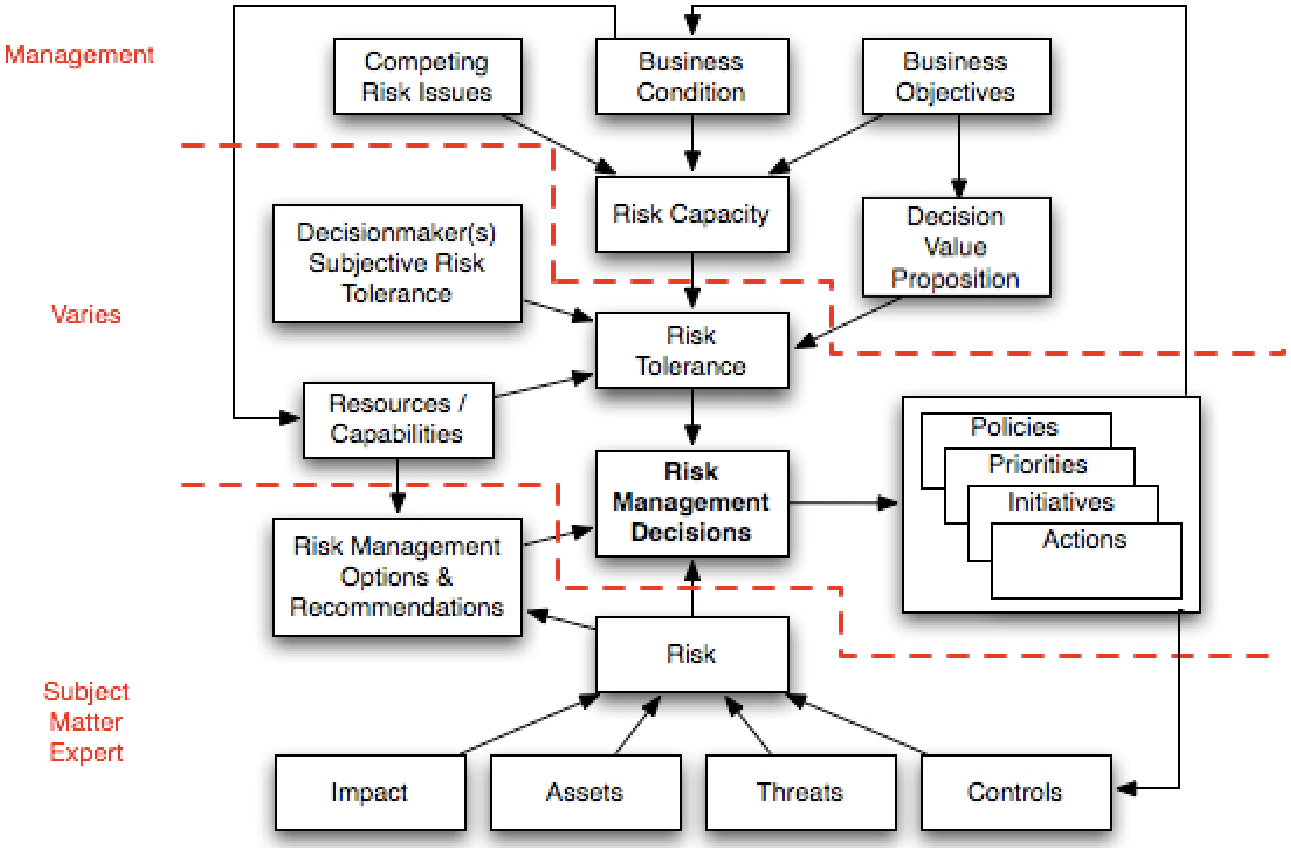
6. Available resources and capabilities help to drive which risk management options are feasible. These resources, of course, are dependent on the organization's condition. Note, too, that resources and capabilities can affect risk tolerance, as an organization with fewer resources for mitigating risk may be forced to accept more risk if, for example, a decision's value proposition is particularly compelling.



7. And finally, the policies, priorities, initiatives, and actions that result from risk decisions will have an effect on risk and the organization's condition (for good or ill). At the very least, expenditures made to manage information risk are no longer available to use on competing risk issues and opportunities.



Okay, if by now you haven't fallen asleep or decided to spend your time elsewhere, I'll tie all this back to the original question of who should be making the decisions regarding information risk.



Carving it up

Using the illustration of the risk decision elements we can draw lines that carve the landscape into three parts:

- Those elements that would appear to belong to business management,
- Those elements that would appear to belong to the subject matter experts (in this case, us), and
- Those elements in the middle that, well, could go either way.

Note that the decision itself falls into the "could go either way" domain, which means I can't give you a definitive, "This is how it should be" answer. What isn't surprising is that who makes the risk decisions will vary from organization to organization. What's unfortunate is that in many companies security leadership believes they are (or should be) empowered to make the major decisions while business leadership believes otherwise. Speaking from painful personal experience, this disconnect can cause significant trouble.

Size matters

Of course what I mean is that the size (significance) of the risk decision also determines who can/should/will make the decision. Business management isn't usually going to be involved in day-to-day operational risk decisions. Furthermore, security management can't personally be involved in each discreet risk decision that takes place throughout the organization (e.g., Clerk: "Hmmm. Should I shred this document, or just chuck it in the trash?"). These day-to-day and discreet risk decisions are where good policies, procedures, and risk awareness education come in.

At the end of the day, decision significance is a continuum rather than a binary or clearly differentiated scale. Consequently, some decisions fall into a grey area regarding who should make what call. For these issues, the question of who should make the decision will vary from organization to organization. You can, however, work with management to come up with some ground rules, for example; policies, policy exceptions, strategic initiatives, and significant expenditures fall into business management's court, and security deals with the rest.

Look again

With regard to discreet risk decisions, take a close look at the risk decision diagram. You'll see that the diagram applies quite well whether we're talking about major strategic decisions or the discreet risk decisions being made by employees countless times each day. The only difference is that, in the absence of a clear understanding of organizational risk tolerance, employees WILL substitute their own views of organizational risk tolerance (or leave it out of the equation altogether). In any event, employees often will be placed in the unfortunate position of having to reconcile organizational risk tolerance with their own conditions/objectives/competing risk issues, etc. (e.g., the question of choosing compliance with security policy over meeting the deadline their bonus is resting on). This highlights the need to be aware of, and manage, issues related to competing individual and organizational priorities.

Something else to think about is that policies and processes will never cover all of the potential risk decisions our employees face. As a result, it's critical that education and awareness efforts go beyond regurgitating policy, and include information that helps employees understand risk and the organization's risk tolerance so that they can make good judgment calls. This better understanding also helps them tolerate those policies they otherwise chafe at.

Things to consider

The simple fact is, security leadership will never know as much about the business-related elements at the top of the illustration, and business management will never know as much about the risk elements at the bottom. Consequently, if security is empowered to make the major decisions, then they need to spend the time and effort to learn as much as they can about the business-related elements. On the other hand, if business leadership is making the major risk decisions, then security must provide clear, unbiased, and useful information so that the decisions are well informed.

For those who are curious, I strongly prefer that business management make the major risk decisions where I work. I'm far more comfortable in my ability to provide them with good risk information and mitigation options than I am in my ability to sufficiently learn and understand the complex business landscape. Besides, when they're the ones who have made the decisions, push-back and arguments are largely eliminated. I've also found that you have far more influence as a trusted advisor than as a combatant.

A decision-maker will to some degree ALWAYS apply his or her own personal risk tolerance to a decision. Consequently, if security leadership has been empowered to make major risk decisions, they should try very hard to be as aware as possible of business management's risk tolerances. If security leadership isn't careful on this, then they will, invariably, run into issues where business management doesn't support security's decisions. And if the misalignment is bad enough (and I've both witnessed this and come close to having it happen to me – long ago) then it can become a "terminal" condition. At the very least it makes the waters far choppier than necessary.

I make it a point to review the risk decision question (and now the diagram) with business management whenever I take a new job or have a new business leader join the organization I work for, even if I'm pretty confident about where they stand. When I've had these conversations it's always generated very productive dialog and has strengthened the relationship.

Jack Jones (CISSP, CISM, CISA) has been employed in technology for the past twenty-four years. He spent over five years as CISO for a Fortune 100 financial services company where his work was recognized in 2006 when he received the ISSA Excellence in the Field of Security Practices award at the RSA Conference. He also has developed and published a sophisticated quantitative risk analysis framework known as Factor Analysis of Information Risk (FAIR). In 2007 Jack was selected as a finalist for the Information Security Executive of the Year, Central United States. He regularly contributes to the Risk Management Insight blog - riskanalysis.riskmanagementinsight.com

Interview with Zulfikar Ramzan, Senior Principal Researcher with the Advanced Threat Research team at Symantec

By Mirko Zorz

Zulfikar Ramzan's current focus includes phishing and fraud, as well as general web security issues, though his professional interests span the theoretical and practical aspects of information security and cryptography. Prior to joining Symantec, Dr. Ramzan held positions at NTT DoCoMo USA Labs, IP Dynamics and Lucent Technologies / Bell Labs. He has co-authored over 30+ published scientific research papers, 15+ patent applications, and one book.

What have been the biggest challenges for you in 2007 so far?

Attackers have been employing so-called blended threats – these are threats that perform multiple malicious activities. For example, a single threat might not only record your keystrokes, but could also be used to send spam from your machine, and set up a backdoor so that an attacker can control the machine later at his or her whim. The spam that is sent might lure the recipient to a web site containing a code snippet that exploits a browser vulnerability to set up a backdoor on their machine. While the specific individual threats themselves are well known, what is unique here is the blending of them into one attack.

This blending suggests that the perpetrators are organized cyber-criminals and are well versed in the different types of attacks that can be mounted. Also, each attack has its own “business model” for the attacker. For example, keystroke loggers are used to steal sensitive data from the victim’s machine, which can later be used in identity theft. On the other hand, if a victim’s machine is turned into a spam zombie, then the attacker can profit by “renting” the machine to a spammer.

By having blended threats, attackers are indicating that they understand these different models, and know how to monetize their efforts accordingly. This behavior is also indicative of professional organized crime as opposed to hobbyists.

What does it entail to be able to predict what kind of threats are about to dominate the mainstream?

There are four high-level approaches to being able to predict what kinds of threats we will be faced with.

First, we constantly monitor malicious activity to see what techniques attackers are using and get a sense of what techniques they might start employing. We find that among attackers, some are more innovative and others just follow the crowd using tried and tested attack methods. Fortunately, the innovative attackers are in the minority.

Second, we also monitor the security research literature to get a sense of what kinds of new security issues we might be faced with in the future. For the most part, attackers tend to do the simplest thing that works, so it's not common to find them implementing the latest concepts that are discussed among researchers.

Third, we perform our own research, especially on new technologies, to get a sense of where they might be vulnerable and what attackers might try. If we come across any serious security threats, we inform vendors so that the technologies may be patched.

Finally, we think about not only what protection gaps exist in our own products, but also about how attackers will react to the countermeasures we put in place. Since Symantec is one of the world's largest software companies and the largest vendor of technologies related to security and reliability, we are very much on the radar screen of attackers. So, when we take any measure, we know attackers are paying attention, and getting ready to plan their next move. Consequently, we spend a considerable amount of effort anticipating that next move and preparing for it accordingly.

NOWADAYS, ATTACKERS ARE CREATING MORE SILENT THREATS.

Is the rising skill level of malicious users becoming a problem when designing countermeasures and security awareness?

We have definitely noticed that attackers have become more skillful, and that malicious code samples have increased in technical sophistication. Awareness has definitely been an issue. It used to be the case that attackers wanted you to know that your machine was infected – primarily since fame was their objective. Nowadays, attackers are creating more silent threats. They are trying not to be noticed. As a result, the general population might not be aware of the kinds of security risks that are out there. It can be a challenge trying to explain the dangers of the threats we've monitored, when they are not as visible.

From a technical perspective, developing countermeasures has become more challenging. But, so far, I think the industry has done an excellent job of finding innovative approaches to address the threats we are seeing. I don't think that there is a silver bullet that can fix every problem we encounter. However, I'm also not convinced that there needs to be one either. The new breed of cyber criminal is financially motivated. Therefore, solutions do not always need to be technically flawless, they just need to render the attack approach unprofitable for the attacker. Nonetheless, we are all still aiming to develop the best solutions possible.

What's your take on the full disclosure of vulnerabilities?

I believe and support responsible disclosure. This practice is what Symantec has followed and we believe it's the best way to serve our customers and protect the Internet community. We support the security community's belief that vulnerability information should only be released to the public once corrective actions have been made and suitable safeguards are available for users of the affected products or in the case a vendor has repeatedly shown a disregard for the identified issue. Symantec is an active member in the Organization for Internet Safety (OISafety) to promote the development and use of responsible disclosure guidelines.

The threat landscape has changed a lot in the last five years. What kind of threats was it most important to protect against before and which ones the in the spotlight now?

It used to be the case that attackers were hobbyists interested in notoriety and infamy. They wanted to infect your machine with some piece of malicious software and made sure that you knew about it. These attackers were likely just interested in being a nuisance more than anything else. A few years ago, we began to notice a shift away from such attackers towards more financially motivated ones. These attackers wanted to put malicious software on your machine that could do things like surreptitiously record your key strokes for the purposes of identity theft and similar acts. Notoriety was no longer a concern. We noticed that these financially motivated attackers started treating their activities as more of a full-time job than as a source of side-income. For example, we observed more activity taking place Monday through Friday, with marked dips on the weekends. Such work habits matched the patterns you might see at a typical corporation. Since then, attackers have also become more organized – working in teams and relying on a fairly evolved underground economy and supply chain. Many aspects of a cyber criminal operation can be easily outsourced. For example, if one wanted to mount a phishing attack, it is possible to purchase a phishing kit with ready-made web pages and sample emails, rent a compromised web server where the pages can be hosted, and even rent a spam zombie from where the phishing emails can be sent out. A list of email addresses can even be purchased. Finally, once credit card or other information is obtained in the attack, it can be sold in the underground economy. So, the phisher need not even worry about how to cash out his proceeds.

Most recently, we are noticing that malicious code is being developed using the traditional software development lifecycle. That means that the malicious code is constantly being made more robust and comes with improved functionality. People who purchase malicious code kits can often expect them to have professional user interfaces and be relatively easy to use. In some cases, malicious code kits that are purchased in the underground market even come with one year of free technical support!

What kind of threat evolution do you expect? What will the future bring?

I think we'll continue to see an increase in the level of professionalism and technical sophistication of the threats in question. I also expect attackers to leverage more creative business models. For example, online gaming environments often have virtual currencies that have real world value. They provide an opportunity for an attacker to not only benefit monetarily, but to also launder money out of the system. Moreover, the legal implications of virtual currency theft are unclear. We have been seeing some attack activity in this area and I expect it to go up. In general, I think attackers will not only continue to "follow the money", but do so in a way that allows them to get the money out safely as well.

Also, I expect that we will see some activity in conjunction with newly released technologies like Windows Vista or the iPhone. However, since attackers are financially motivated, we may not see much activity until these technologies become more dominant in the marketplace. Attackers prefer going after targets that provide the most bang for the buck.

In addition, we have been seeing some activity that is highly targeted – going after high net-worth individuals. I expect such instances to increase as well. Targeted attacks often leverage information gathered from multiple sources and as data breaches and such become more common, there will be more information available for attackers to choose from. In general, contextual information can dramatically increase the success rate of attacks. After all, you are more likely to open an attachment sent from a friend than you are to open one from a stranger. If an attacker can figure out who your friends are, then they can forge their email address when trying to attack you. Nowadays, figuring out who your friends are is pretty simple – most people publicly reveal that information on social networking sites like Friendster, Facebook, MySpace, and others. I expect to see attacks that leverage these public sources as well.

Software spotlight

WINDOWS - Cryptainer LE
http://www.net-security.org/software.php?id=586

This tool enables you to secure your data and ensure absolute privacy. Cryptainer LE uses 128 bit encryption, creates multiple encrypted containers (vaults) on your hard disk.

LINUX - Dropbear SSH Server
http://www.net-security.org/software.php?id=490

Dropbear is an SSH 2 server, designed to be usable in small memory environments.

MAC OS X - SafariSafe
http://www.net-security.org/software.php?id=677

SafariSafe is a simple application to temporarily move all of your Safari settings to a safe place, and lock your keychain.

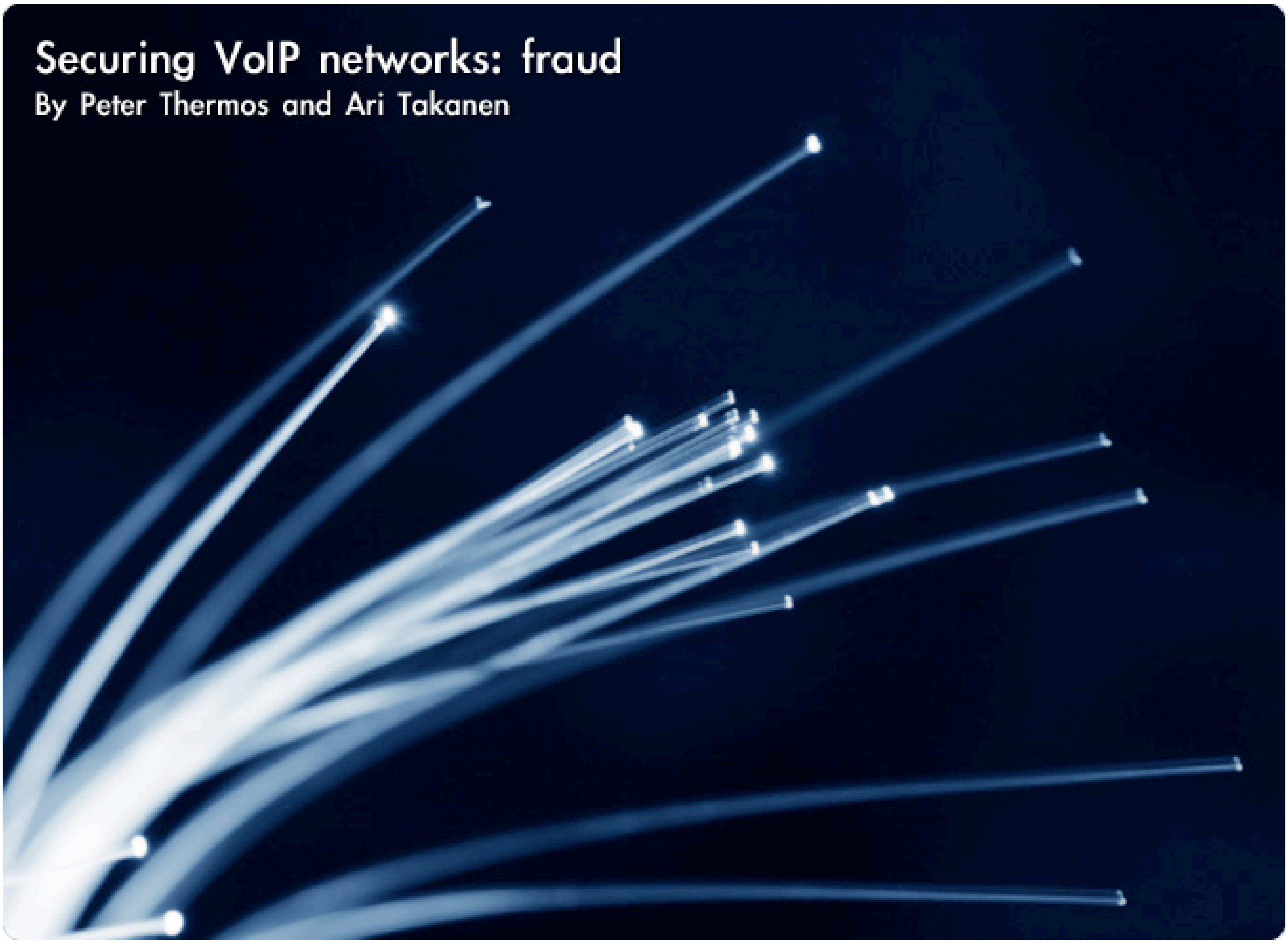
WINDOWS MOBILE - WiFi Graph
http://www.net-security.org/software.php?id=634

WiFi Graph let you spot neighboring Wireless LAN access points and their connectivity. With proprietary scanning technology, access point information is updated every second so you can always rely on it. IT security professionals can also use our XML-based logs to analyze the invisible network.

To submit a software for consideration e-mail software@net-security.org

Securing VoIP networks: fraud

By Peter Thermos and Ari Takanen



As technology evolves, fraud schemes are also made easier to carry out at a higher frequency. In addition, the convergence between circuit-switched and packet-based networks will increase the opportunities for fraud.

In 2004, the FBI reported an increase in online fraud from 2003 by 64 percent. The total loss amounted to $68.14 million, with Internet auction fraud being “by far the most reported offense.” Telecommunications fraud has been one of the primary concerns of telecommunications carriers and service providers for many years. Generally, fraud in telecommunication networks (that is, wireline and cellular) has an annual growth of about 10 percent on average.

A worldwide telecom fraud survey that was conducted by the Communications Fraud Control Association in 2003 identified telecom fraud losses to be $35 to $40 billion. It has been reported that the average loss for a service provider is estimated to be between 3 percent and 8 percent annually. In addition, it is estimated that there are a little more than 200 variants of telecom fraud, and it is anticipated that this number will increase with the growth of next-generation networks including VoIP and IMS.

Today, network providers that maintain a reasonable IP backbone can offer competitive VoIP services. This includes not only incumbent telcos, but also cable operators and Internet service providers. Therefore, deployment of packet-based multimedia applications such as VoIP, IPTV, and others has become a priority to maintain competitiveness. The demand to market quickly inhibits the implementation of adequate security controls. In addition, the network architecture changes dynamically to accommodate new services, applications, and billing methods.

All these variables (new and complex technology, new services, new billing methods, and time to market) provide a fertile ground for fraud and criminal activity that will propagate at a higher rate compared to the past.

Generally, one factor that aids in accelerating fraud activity is the availability of tools (software, hardware, or the combination of both) that lessen the technical competence required to carry out the fraud and provide the means to easily and continuously replicate the process.

VoIP fraud introduces a new challenge for the service providers because of many factors, including the following:

- Complexity of the technology increases the opportunity for security inconsistencies and oversight.
- New technology, and therefore new security limitations and vulnerabilities, are introduced.
- Time to market to remain competitive suppresses the need to deploy proper security controls.
- Billing methods may vary based on multimedia content, QoS, usage, or other matrixes, which expands the room for error and opportunity to manipulate billing codes or processes.

Fraud introduces socioeconomic issues by affecting the health of the provider's business and operations, which in turn may affect operating costs and to some extent consumer pricing. Although fraud has been a telecommunication provider issue, with the general increase of VoIP deployments, it will expand to enterprise network owners, too. External and internal attackers will try to gain access to critical components such as the IP-PBX or signaling gateways to make fraudulent calls, reroute calls to support money-making schemes, or methodically disrupt communications for extortion.

An attacker may use traditional methods to defraud VoIP services, such as social engineering or identity theft. For example, one of the methods used by criminals to defraud telecommunication services is to impersonate an existing subscriber by obtaining personal information of a subscriber (for example, name, address, and Social Security number) and requesting new services, which are abused and later abandoned.

The more technically savvy attacker can use a single vulnerability or a combination of vulnerabilities to obtain services fraudulently. These vulnerabilities may exist because of poor security controls on infrastructure components (that is, SIP proxy servers, H.323 gatekeepers, SBCs), insecure software implementations, or protocol limitations.

Types of Fraud

There have been various ways to defraud telecommunication services, which are discussed next. It is necessary to understand the types of fraud methods that exist to place them in the context of VoIP and essentially in NGN and derive possible new fraud scenarios. According to historical data, there are approximately 200 types of known telecommunication fraud. Some of these include subscription fraud, dial-through fraud (manipulation of the PBX), freephone fraud, premium-rate service fraud, handset theft, and roaming fraud. Generally the types of fraud can be categorized as fraud that targets the process (that is, subscription, superimposed)29 and fraud that targets the technology (that is, autodialers, unauthorized access). Here we discuss some of the most commonly experienced.

Subscription fraud is committed by purchasing services using falsified identity information. There are numerous ways that subscription fraud can be carried out. The purchased services may be sold to others or used by the criminals to run up high toll charges and collect the money from the targeted telephone company. The objective of the perpetrator is to use the service and run up high charges and later abandon the account or use the subscription to collect toll money from the telco. For example, someone can subscribe to a telephone service at a company in the United States using falsified or stolen identity information. At the same time, the perpetrator may have set up an account in another country for which he charges $5 per minute for incoming calls. This allows making calls from the United States and getting charged outrageous tolls on the U.S. account. The perpetrator collects the money from the local telco for the incoming calls, but obviously doesn't pay the charges on the U.S. account (thus leaving the telco in debt). Although this scheme has been very costly for telcos, it provides several indicators that can be used in fraud detection, which are discussed in later sections.

Superimposed fraud is caused by fraudsters using another user's subscription without authorization. All the toll charges are billed to the account of the unsuspecting victim. The fraud is committed by having access to the user's stolen equipment (for example, cell phone), equipment cloning, or the use of personal-identifiable information such as a calling card or subscription plan information with the telco.

Detecting this type of activity is difficult but not impossible. Anomaly-detection methods can be used in fraud management, which we discuss below. Unauthorized access is one of the fundamental techniques used for many attacks, including committing fraud. Gaining access to billing systems, telephone switches, or other infrastructure components allows an attacker to manipulate the configuration or data (that is, call detail records) to avoid charges. Unauthorized access takes advantage of vulnerabilities that may exist in the software that runs on the infrastructure components, poor configuration, or lack of proper security controls.

Gaining access to billing systems, telephone switches, or other infrastructure components allows an attacker to manipulate the configuration or data to avoid charges.

Auto-dialers are programs designed to make automated calls to a list of phone numbers or a telephone exchange. The auto-dialers are used by tele-marketers to call potential customers and sell their services and by phreakers to identify toll-free numbers or modems attached to systems and ultimately attempt to gain unauthorized access. Auto-dialers are also used as a mechanism to carry out fraud. The perpetrator claims to be a customer-owned coin-operated telephone (COCOT) vendor. He then connects an auto-dialer to what should have been a payphone line and initiates war dialing on an assorted list of toll-free numbers (that is, 1-800 in the United States).

Because the calls are made to 800 numbers, the charges are reversed, and therefore the called parties (companies that own the 800 number) are forced to reimburse the fraudulent COCOT provider for "calls received from a pay-phone."

Other fraud schemes include pre-paid calling cards that use passcodes that can be stolen and then used to make fraudulent calls, telemarketing that attempts to sell services to vulnerable victims (for example, elderly), and forced calls to service numbers (for example, 809, 876-HOT, 900) that are purposefully overpriced (and the owners reside in countries where such practice is not legally restricted; for example, the Caribbean, Jamaica, and elsewhere).

Fraud in VoIP

It is expected that VoIP providers will experience new types of fraud. Some schemes will be able to be listed under the known categories, but there will be others that will require new categorization and probably new detection and mitigation techniques.

One of the fundamental issues is the fact that the signaling in VoIP is in-band. This means that voice and control messages are not isolated. Although this practice was performed in the older days of the PSTN, when CAS (Common Associated Signaling) was used, it was terminated and a new system emerged, the CCS31(Common Channel Signaling), in which control messages are sent out of band. In the older system (CAS), it was possible to place fraudulent calls because of the ability to send voice and generate control signals over the same line. In CCS when someone makes a call, he receives only a dial tone, without having any control over the signaling. All the control messages to set up and tear down the call occur within the network separately from the user's communication line.

Another area of concern is the architecture of VoIP. Typically, VoIP components (that is, SIP proxies, DNS servers) reside on networks accessible from the Internet and therefore exposed to attack. VoIP service providers may not necessarily manage the Internet connection of their subscribers, and therefore all signaling and voice traffic from the end user's device will traverse one or more foreign networks. This exposes the subscriber and the service provider to various threats, including eavesdropping and unauthorized access, which can support fraud activities. For example, an attacker may exploit a vulnerability in the subscriber's residential VoIP gateway that will allow capturing credentials that can be used to gain access to the provider's network and make fraudulent calls.

Fraud Through Call-Flow Manipulation

Figure 1 shows an example in which implementation vulnerability can be used to defraud a VoIP service. The vulnerability takes advantage of how SIP signaling messages are processed by the SIP proxy and the billing system. Typically, a SIP proxy considers that a session between two users has been set up when the three-way handshake is completed (INVITE, OK, ACK messages). Figure 1 depicts a typical SIP handshake.

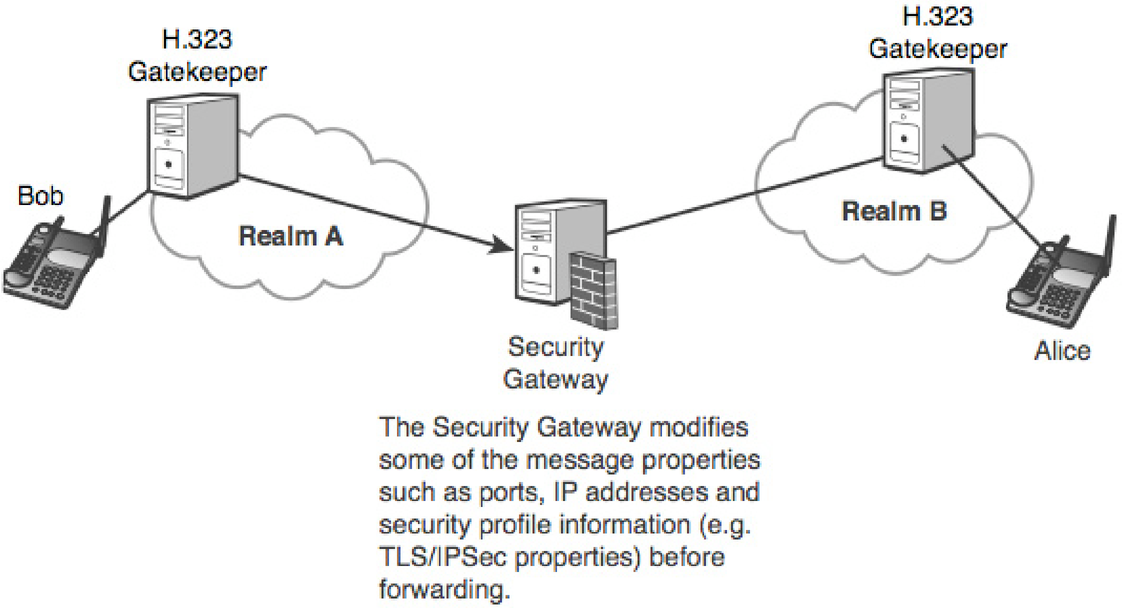

H.323
Gatekeeper
H.323
Gatekeeper
Bob
Realm A
Realm B
Security
Gateway
Alice
The Security Gateway modifies some of the message properties such as ports, IP addresses and security profile information (e.g. TLS/IPSec properties) before forwarding.

Figure 1 - Typical three-way SIP handshake.

Bob wants to talk to Alice, and when he dials the digits, his phone generates an INVITE message that is sent to his local SIP proxy. Bob's proxy performs a lookup to determine to which proxy it needs to send the INVITE to reach Alice's proxy. Upon determining the IP address of the proxy that serves Alice, it forwards the INVITE, and Alice's proxy forwards the INVITE to Alice's phone. When Alice answers the phone, an OK response is sent to Bob's phone to indicate that Alice has accepted the call. At that point, Bob's phone sends an ACK response, which indicates that the session has been established and the two users can communicate. Notice that all the messages are propagated through both proxies A and B, and therefore there is a record of the messages that have traversed the proxies. The records that are created on the proxies are critical for providing billing and service-usage information. If this information is corrupted or not recorded accurately, it impacts the service provider's billing process.

One way to defraud a VoIP service provider is by manipulating the call flow between the two end points. It is possible to establish a call between two end points and avoid toll charges by manipulating the SIP message sequence.

Let's assume that Bob has the ability to manipulate the message flow of his SIP phone (for example, by manipulating the runtime code or proxying the SIP messages through another device). In this case, he will send the SIP INVITE to contact Alice. The INVITE request will propagate through the intermediate SIP proxies A and B and eventually will reach Alice. When Alice answers the phone, an OK response is sent back to Bob's SIP phone. At this point, Bob knows that Alice has answered. In essence, Bob can start sending voice to Alice's phone without having to send the ACK response.

Figure 2 on the following page demonstrates this scenario.

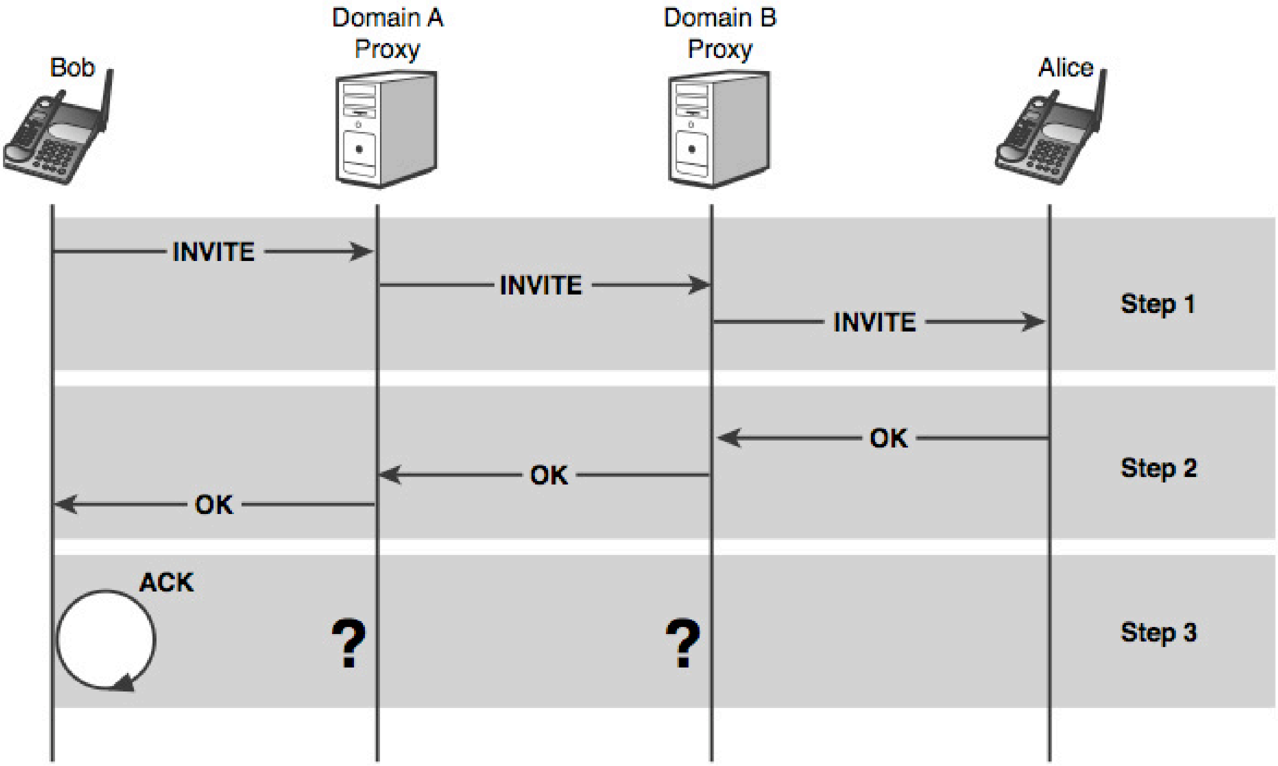


Figure 2 - SIP message-suppression attack used for service fraud.

In this case, the ACK response is suppressed and the intermediate proxies (A and B) assume that the call was not established and therefore do not record it (see Figure 2). Therefore, it will not be reflected in the billing records either. Depending on the implementation, Alice's phone may have to be programmed to ignore waiting for an ACK and to accept media streams on the preallocated ports that were indicated in the OK response.

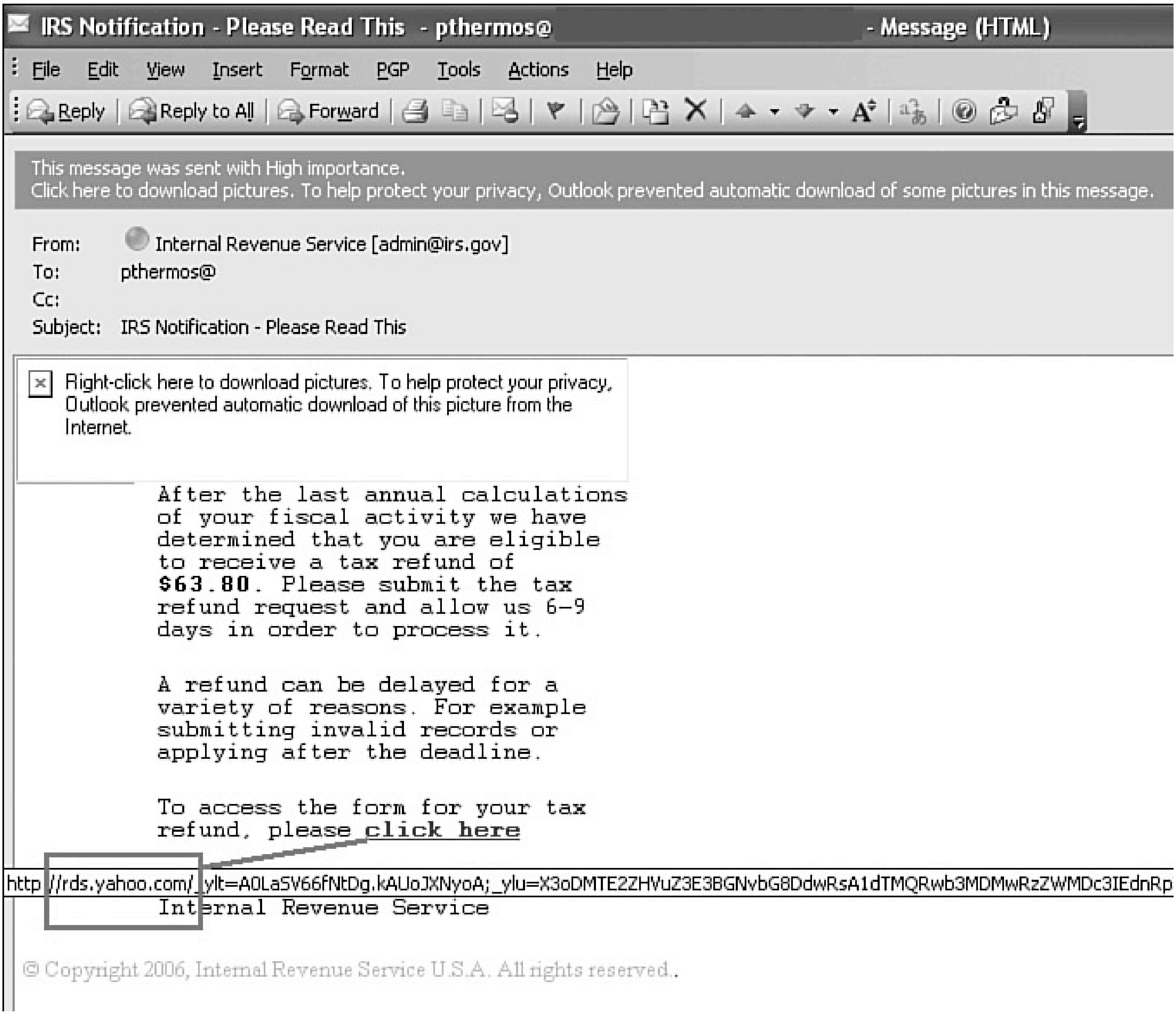
One approach that service providers take to protect against this attack is to start billing when the OK is sent back from the called party. Although this provides some protection, it might not stop emerging attacks that manipulate the call flow or signaling messages to bypass billing.

Phishing

The term phishing refers to an attacker sending masqueraded email messages to unsuspecting users to lure them into disclosing confidential or personal information, such as account credentials. The email message has the same look and feel of a legitimate message originating from an organization that the user has a prior relationship with, typically a financial institution or online merchant (for example, Bank of America, IRS, eBay, Amazon).

Figure 3 shows an email message that appears to originate from the IRS (Internal Revenue System). The email message can be crafted to appear as if it originates from a specific organization that maintains private user information such a financial institution.

The message urges the user to visit the institution's online system to verify credentials, claim a balance, or dispute a charge. The content of the message is formatted using HTML, which helps the attacker to obfuscate the real URL that the user is asked to follow to verify his or her credentials. The highlighted "click here" text appears as an HTML link as a convenient way for the user to connect to the online system and proceed with the verification of credentials. In Figure 3, the highlighted link indicates that the actual URL resolves to the rds.yahoo.com domain, which is clearly not an IRS system. In addition, the URL contains the path to a script that prompts the user to enter his or her credentials, such as Social Security number, user ID and password, credit card number, and so on). When the user follows the URL, he is prompted to enter his credentials, which will be captured by the attacker. The credentials may be logged in a file, sent to an email account, or posted to another Web site or IRC channel.


IRS Notification - Please Read This - pthermos@ [redacted] - Message (HTML)
File Edit View Insert Format PGP Tools Actions Help
Reply Reply to All Forward

This message was sent with High importance.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From: Internal Revenue Service [admin@irs.gov]
To: pthermos@
Cc:
Subject: IRS Notification - Please Read This

☒ Right-click here to download pictures. To help protect your privacy, Outlook prevented automatic download of this picture from the Internet.

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of **$63.80**. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please **click here**

http://rds.yahoo.com/_ylt=A0LaSV66fNtDg.kAUoJXNyoA;_ylu=X3oDMTE2ZHVuZ3E3BGNvbG8DdwRsA1dTMQRwb3MDMwRzZWMDc3IEdnRp

Internal Revenue Service

© Copyright 2006, Internal Revenue Service U.S.A. All rights reserved..

Figure 3 - Sample “phishing” email message.

The same approach can be using VoIP communications. An attacker can lure unsuspecting victims into calling a number managed by the attacker. The email message can be sent to users asking them to call an 800 number. Figure 4 shows the steps used in this attack. The first two steps can be performed simultaneously or in either order. In our example, the attacker has first analyzed the target company’s interactive voice system and creates an exact replica. In the next step, an 800 number is obtained by a VoIP service provider (it provides a layer of believability to the spoofed message being sent because users are accustomed to calling toll-free numbers to contact customer service). In addition, the cost for a VoIP toll-free number is relatively insignificant. The next step is to craft and send an email message that instructs recipients to call the 800 number and verify their credentials for the targeted institution. If recipients are convinced to call the 800 number, they will go through the prompts and disclose their credentials. The spoofed system can terminate the victim’s call by responding with a polite message such as “Thank you for verifying your information with Big International Bank!” and hanging up the call. And the attacker will have recorded the information on his or her system. It is expected that VoIP-related phishing attacks will become apparent during 2008 or 2009.

Another variation of this attack is to embed a SIP URL rather than an HTTP URL in the email message. This will work only in cases in which the user’s system has the ability to place VoIP calls using SIP URLs.

Another attack is to invoke the soft phone that resides on a victim's system by using a command in the URL link, such as the following (see Figure 5):

```
C:\Program
Files\CounterPath\X-Lite>x-lite.exe
--help - dial=sip:7325551212
```

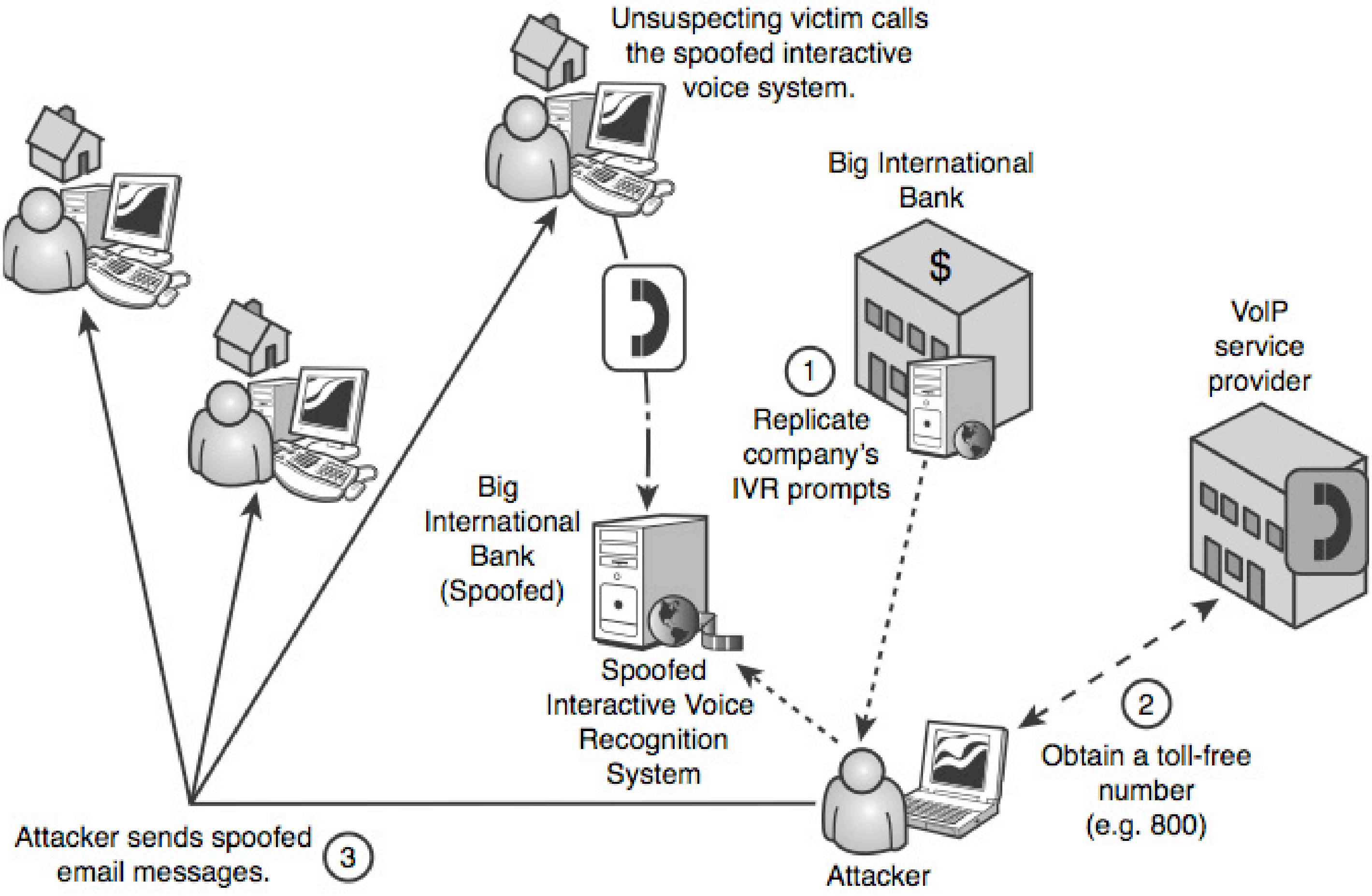
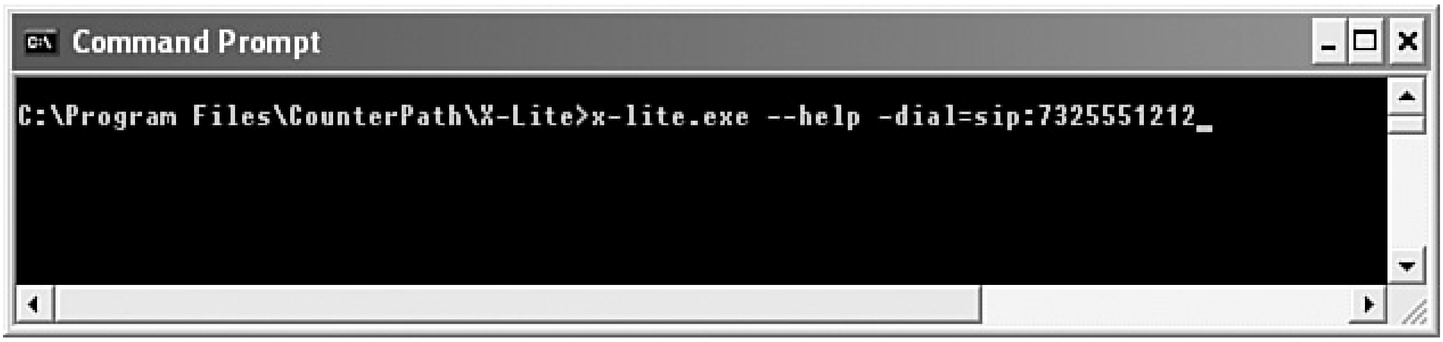

Unsuspecting victim calls the spoofed interactive voice system.
Big International Bank
$
1
Replicate company's IVR prompts
VoIP service provider
Big International Bank (Spoofed)
Spoofed Interactive Voice Recognition System
2
Obtain a toll-free number (e.g. 800)
Attacker sends spoofed email messages.
3
Attacker

Figure 4 - VoIP phishing attack.



```
C:\Program Files\CounterPath\X-Lite>x-lite.exe --help -dial=sip:7325551212_
```

Figure 5 - Invoking a soft phone from a command line or an attack script.

The first line of defense is user awareness. Organizations should educate their users of the potential of such attacks. From a technological perspective, a mutual caller ID authentication mechanism should be established. Such an enhancement will require the development of an ITU or IETF standard. The proposed standard will require that the called institution authenticates itself to the user by announcing to the user a piece of information that will be known to the institution and the user only. For example, the institution can prompt the user to select from a list of choices a private piece of identifying information such as the last four digits of the respective account or Social Security number (for example, “Does your account number with us end in 6789, 1111, 4343, or 3232?”).

The user can select the correct response, which is already known to the user and institution.

Although this attack has several technical parameters, it is categorized under fraud because it is mainly used to obtain a user's credentials for identity theft and to perform fraudulent transactions such as unauthorized purchases, money transfers, or withdrawals.

Fraud Management

Fraud management in VoIP requires a multidimensional approach because of the complexity of the technology and the variation in applications and services. To effectively combat fraud in VoIP networks, the following should be considered:

- Incorporate fraud control requirements in new service offerings as part of the product development life cycle.
- Define fraud control requirements in the early stages of a product offering to minimize potential loss due to fraud and help streamline the fraud management system to detect behaviors that violates the defined requirements. This proactive measure helps minimize costs associated with later efforts to manage service fraud at the time of occurrence.
- Deploy a VoIP fraud management system to assist in recognizing suspicious activity patterns. Several vendors offer fraud management systems for VoIP. Before selecting and deploying such as product, consider the following:

➡ Security features offered by the system, such as role-based access controls (that is, administrator, analyst, manager), secure remote access (that is, SSL/SSH), and data integrity.

➡ Pattern-matching capabilities (that is, granularity of configurability, elimination of false positives).

➡ Detection and pattern-recognition capabilities (that is, event- or rule-based detection).

➡ Integration and maturity curve (that is, the amount of time it takes for the analysis engine to "learn" network traffic behavioral patterns).

➡ Alert mechanisms (that is, console, pager, remote management station).

➡ Performance capabilities and limitations (that is, analyzing large data sets within a reasonable amount of time).

➡ Reporting capabilities (that is, categorizing and prioritizing events).

➡ Training and learning-curve requirements.

It is important to note that deploying a fraud management system will not guarantee minimization of fraud losses unless the deployment of the fraud system has been appropriately planned and implemented.

A critical aspect for deploying a fraud management system is to identify requirements for managing and administering the system, along with integrating it into the current infrastructure. Telecommunication service providers purchase fraud management systems without performing proper evaluation, which leads to poor implementation and higher maintenance costs.

Identifying an infrastructure's capabilities and integrating associated control mechanisms in the fraud management plan can help manage and suppress fraud activity. For example, enforcing bandwidth limiting for specific subscribers, performing message inspection to identify suspicious activity, and implementing access control mechanisms (that is, authentication servers, session border controllers, firewalls).

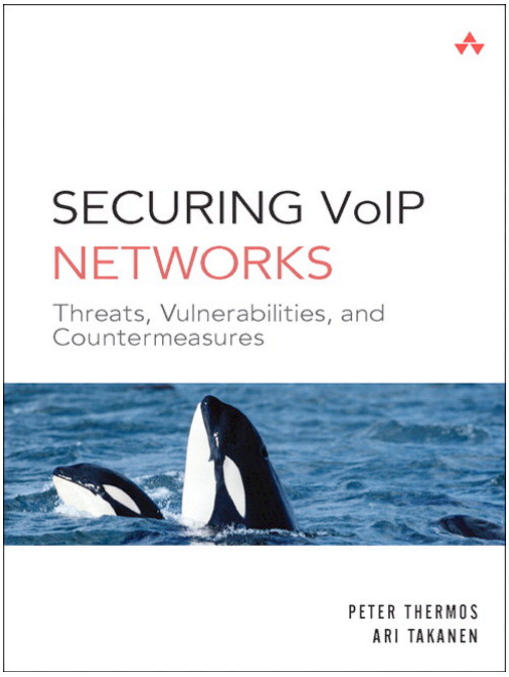
Some large telcos have established fraud management and reduction teams that focus on defining and implementing the company's strategy for fraud management. The team is responsible for defining requirements to manage fraud, coordinating data collection and analysis, and promoting awareness. For smaller organizations, such as enterprise networks, fraud management is an integral responsibility of the security or network engineering team, which may or may not possess the appropriate knowledge and skills to manage fraud and therefore require the help of external subject matter experts.

In either case, organizations of all sizes should maintain a mechanism for disseminating information about fraud activity to other organizations through various channels (for example, associations or online forums) or contacting the local and federal law enforcement agencies. This mechanism helps raise awareness and minimize the propagation of fraud activity.

Peter Thermos, Principal, Telcordia Technologies, has been providing consulting in the area of information security to commercial and government organizations for more than a decade.

Ari Takanen is a founder and CTO of Codenomicon Ltd. He is a distinctive member of the global security testing community and a regular speaker at various testing and security conferences.

This article is an excerpt from the Addison-Wesley book “Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures” and you can find out more about it in the “Latest addition to our bookshelf” section in this issue of (IN)SECURE.



PCI DSS compliance: a difficult but necessary journey

By Andre Muscat

The need to comply with the Payment Card Industry Data Security Standard (PCI DSS) has been a rude wake up call for thousands of companies who believed their networks are secure and safe from security breaches.

This standard is a set of network security requirements agreed upon by five of the major credit card companies in an attempt to stem the growth of credit card fraud around the world and to give a common interpretation of what security is all about. Since PCI DSS was launched, it has helped to expose serious security shortcomings, companies' failure to follow security best practice and a general lack of awareness of the security threats facing organizations today.

The statistics reveal a worrying increase in the level of identity theft and credit card fraud. According to a Federal Trade Commission report in January 2007, 25% of reported identity theft in 2006 was credit card fraud. Considering that more than $49 billion was lost by financial institutions and businesses in that year due to identity theft, and $5 billion lost by individuals, credit card fraud is digging deep into everyone's pockets. E-commerce fraud is also on the rise, reaching $3 billion in 2006, an increase of 7% over 2005.

A growing sense of urgency to meet these requirements was spurred by TJX Companies Inc.'s loss of 45.7 million records containing customer personal account information as well as 455,000 merchant details over an 18-month period. Although the TJX breach is considered to be the biggest in US history it is not the only one. According to the Privacy Rights Clearinghouse, between 1 January 2005 and August 2007, more than 159 million records containing sensitive personal information have been involved in security breaches. The actual figure is probably higher because many cases are either under-detected or they are not reported at all.

Large retailers like TJX are not the only organizations being targeted. Public attention may be focused on high-profile data losses, but experts studying financial fraud say hackers are increasingly targeting small, commercial websites as well! In some cases, criminals were able to gain real-time access to the websites' transaction information, allowing them to steal valid credit card numbers and use them for fraudulent purchases. Although small businesses offer fewer total victims, they often present a softer target; either due to flaws in the e-commerce infrastructure being used, or due to over-reliance on outsourced website security or simply due to the false belief that their existing security set-up is adequate.

Knee-jerk reaction?

The PCI DSS is not the result of a knee-jerk reaction to an increase in security breaches but it is a studied approach to data security taken by each of the card companies. Before 2004, American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International had a proprietary set of information security requirements which were often burdensome and repetitive for participants in multiple brand networks.

Seeing the need for greater cohesion and standardization, these associations created a uniform set of information security requirements that became known as the PCI Data Security Standard (PCI DSS), governing all the payment channels: retail, mail orders, telephone orders and e-commerce.

THE PCI DSS IS NOT THE RESULT OF A KNEE-JERK REACTION TO AN INCREASE IN SECURITY BREACHES BUT IT IS A STUDIED APPROACH TO DATA SECURITY

Deadlines looming

For more than two years, credit card companies have been encouraging retailers to comply with the strict set of 12 requirements that are aimed at securing cardholder data that is processed or stored by them. Unfortunately, with two deadlines looming – 30 September and 31 December 2007 for Level 1 and Level 2 US merchants – it seems that many companies will not be ready in time. Even with a last minute push, it is highly improbable that retailers – large or small – have the time or the resources to become compliant in such a short-time frame. Most companies, especially in the SMB market, want to become compliant but they are still struggling to introduce basic security practices let alone implement all the systems needed to become compliant. The most recent compliance statistics from Visa for the month of July indicate an improvement but they are far off the targets that Visa and the other card companies hoped for.

According to figures for July, 40% of Level 1 retailers were compliant, up from the 35% compliance rate in May 2007. With the somewhat smaller Level 2 retailers, the July figures showed a 33% compliance rate – up from 26% in May – and the smaller Level 3 retailers showed 52% compliance, just slightly up from the 51% that Visa reported for that group in the same month. Visa did not release figures for Level 4 retailers; however it said compliance remained low.

Such a low compliance rate – after more than two years of preaching by the credit card companies – is possibly due to three reasons. First, some companies have taken a very laid-back approach to the issue, realizing only recently that the credit card companies mean business. Now, they are rushing to comply by the deadline, suddenly aware that they have a massive task ahead of them. Second, many small and medium sized companies do not have the resources or the finances to invest in the more personnel or a technology solution to meet the PCI requirements. Third, some retailers have complained that the standard does not distinguish between retailers on the basis of their size

According to the Retail Industry Leaders Association (RILA): "Some PCI requirements are vague. Some are unattainable. Retail companies […] cited numerous examples of low-result PCI requirements, one-size-fits-all rules that don't work for various kinds of retail formats.”

RILA has argued that although there is universal support for the goals and objectives of PCI and its efforts at making payment systems more secure, the standard’s ‘one size fits all’ framework is imposing unrealistic hardships on smaller retailers and it does not "appreciate the practical staffing flexibility that retailers need".

While some of the PCI requirements may be open to interpretation, it is also true that the PCI DSS standard is one of the most robust and clear when compared to other compliance regulations such as Sarbanes-Oxley. PCI is not only the least ambiguous of the lot but it is also the only standard that has gained universal approval.

What is the PCI standard?

The PCI standard is not rocket science and neither does it introduce any new, alien concepts which systems administrators should adopt; on the contrary it is an enforcement of practices that should already be in force on all corporate networks. Although PCI DSS was developed with the protection of cardholder data in mind, more than 98% of the requirements apply to any company that needs to secure its network and its data.

In essence, PCI DSS comprises 12 distinction standards that are designed to 1) Build and maintain a secure network, 2) Protect (cardholder) data in transit or at rest, 3) Maintain a vulnerability management program, 4) Implement strong access control measures, 5) Regularly monitor and test your IT infrastructure and finally, 6) Maintain an information security policy.

The table below shows a breakdown of each category and what companies need to do to become compliant.

The PCI DSS requirements

Often referred to as the 'digital dozen', these define the need to:

Build and maintain a secure network
1: Install and maintain a firewall configuration to protect cardholder data
2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data
3: Protect stored cardholder data
4: Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program
5: Use and regularly update anti-virus software or programs
6: Develop and maintain secure systems and applications

Implement strong access control measures
7: Restrict access to cardholder data by business need-to-know
8: Assign a unique ID to each person with computer access
9: Restrict physical access to cardholder data

Regularly monitor and test networks
10: Track and monitor all access to network resources and cardholder data
11: Regularly test security systems and processes

Maintain an information security policy
12: Maintain a policy that addresses information security for employees and contractors

There are three stages that each and every merchant or provider must go through to become compliant.

First, they are required to secure the collection of all log data and ensure that it is in tamper-proof storage and easily available for analysis. Second, companies must be in a position to prove they are compliant on the spot if they are audited and asked to present evidence that controls are in place for protecting data. Third, they must have systems in place, such as auto-alerting, which help administrators to constantly monitor access and usage of data. These systems must enable administrators to receive immediate warnings of problems and be in a position to rapidly address them. These systems should also extend to the log data itself – there must be proof that log data is being collected and stored.

The requirements make a clear distinction between merchants and service providers and what they need to do to become compliant. All merchants that acquire payment card transactions are categorized in 4 levels, determined by their number of annual transactions:

- Level 1: Merchants with more than 6 million card transactions & merchants which cardholder data has been compromised
- Level 2: Merchants with card transactions between 1 and 6 million
- Level 3: Merchants with card transaction between 20,000 and 1 million
- Level 4: All other merchants.

These levels determine the validation processes that a merchant must undertake in order to achieve and maintain compliance. For example, Level 1 merchants must carry out an annual on site security audit and quarterly network scan. On site security audits are performed by a Qualified Security Assessor (QSA). On the other hand, level 2, 3, 4 merchants must fill in an annual self assessment questionnaire and carry out a quarterly network scan. The self assessment questionnaires are compiled in-house by the merchant while the network scans are performed by an approved scan vendor (ASV). Examples of merchants include online traders such as Amazon.com, Wal-Mart retail outlets, universities, hospitals, hotels, restaurants, petrol stations and so on.

Services providers, which include payment gateways, e-commerce host providers, credit reporting agencies and paper shred companies, are categorized in three levels:

- Level 1: All payment processors and payment gateways
- Level 2: All service providers not in level 1 but with more that 1 million credit card accounts or transactions
- Level 3: Service providers not in Level 1, with fewer than 1 million annual credit card accounts or transactions.

Becoming PCI DSS compliant requires these businesses to fulfill and demonstrate compliancy with all the 12 requirements as follows: Level 1 & 2 service providers must pass an annual on site security audit and quarterly network scan, while Level 3 service providers need to fulfill an annual self assessment questionnaire & quarterly network scan. Self assessment questionnaires are compiled in-house by the service provider and network scans need to be performed by an approved scan vendor (ASV).

It is also in the own interest of acquiring banks to ensure their merchants are aware and compliant to PCI DSS. Acquiring banks are the main actors that build up the line of trust between card companies and merchants and they are also the ones that end up directly in the line of fire of credit/debit card companies whenever one or more of their merchants suffer a breach. To maintain a successful and healthy business relationship with card companies, acquiring banks must ensure that their merchants are adequately protected – by being PCI DSS compliant. Similarly, merchants and service providers are expected to demonstrate their level of compliancy to PCI DSS. This helps to maintain a healthy business relationship with acquiring banks and to avert non-compliance liabilities.

Although acquirers are not currently mandated to carry out any specific PCI DSS validation or certification process, they are still required to be PCI DSS compliant.

The cost of non-compliance

Level 1 merchants have until 30 September 2007 and level 2 merchants have until 31 December to become compliant otherwise they risk hefty fines, possible law suits and loss of business and credibility. The consequences can be serious because apart from card companies imposing fines on member banking institutions, acquiring banks may in turn contractually oblige merchants to indemnify and reimburse them for such fines. Fines could go up to $500,000 per incident if data is compromised and merchants are found to be non-compliant. In a worst case scenario, merchants could also risk losing the ability to process customers' credit card transactions.

Furthermore, businesses from which cardholder data has been compromised are obliged to notify legal authorities and are expected to offer free credit-protection services to those potentially affected. It is also important to note that if a merchant in level 2, 3 or 4 suffers a breach, he will then have to fulfill the requirements for PCI DSS compliancy as if it were a level 1 merchant.

Lesson to be learnt

Achieving compliance to the PCI Data Security Standard should be high on the agenda of organizations that carry out business transactions involving the use of credit cards. Organizations cannot continue to give so little importance to security nor adopt the macho attitude, ‘it can’t happen to me’. This is exactly what hackers and fraudsters want to hear. Implementing software tools for log management, vulnerability management, security scanning and endpoint security will go a long way towards helping you achieve compliance. However, the story does not end there. Just because a merchant receives a PCI stamp of approval, he simply cannot sit back and relax.

PCI compliance is but the beginning of a continuous process that requires regular monitoring of the security health status of the merchant’s network. PCI DSS is not a one-off certification that stops with the Qualified Security Assessor (QSA) confirming you are compliant, as some merchants may think. Becoming PCI compliant means that you have reached an acceptable level of security on your network but it does not mean that from then onwards your network is secure and cannot be breached. Maintaining PCI DSS compliancy status is just as, if not more, important.

PCI DSS compliance is a long-term journey, not a destination. And this is something that all merchants need to understand irrespective of size or business. It is a cost of doing business, granted. Yet, the cost of compliance is a lot lower than having to pay $500,000 in fines and losing your goodwill and credibility if your network is breached!

Andre Muscat is Director of Engineering at GFI Software – www.gfi.com

www.net-security.org
Get up-to-date security information and stay ahead of the storm.

A security focus on China outsourcing

By Richard Lawhorn

India based outsourcers are starting to reduce their costs by outsourcing your BPO process to China to remain cost competitive and offset client defection.

Business process outsourcing (BPO), such credit card transactions, medical claims data entry and financial transactions, has been around for a number of years. The act of outsourcing these functions offshore to India has become increasingly more viable since a great amount of progress has been achieved in developing the information security framework to protect customer data. Many of the risks in outsourcing to India based companies have been mitigated through trial and error along with the adoption of best practices emerging from all parts of the globe.

Over the past 7-10 years, many security risk analysis and reviews have resulted in controls being implemented in most facets of security: administratively, physically and technically. Contracts now have the appropriate language to protect sensitive data and physical security measures have been built to align with the client's company policies and standards. The technical measures continue to build upon a strong foundation built in partnerships with government and outsourcing firms. As we gain the benefits of this maturing environment, it becomes increasingly challenging for the India based outsourcers to remain competitive in the world economy. Many outsourcers realize this issue and have turned to China for the answers. As businesses attempt to keep variable cost structures intact and operational costs down, China presents itself favorably. India based outsourcers are starting to reduce their costs by outsourcing your BPO process to China to remain cost competitive and offset client defection. This change allows them to remain competitive in the world economy but this places a big question back on the security risks we have started to overcome with India over the past few years.

No matter which way this outsourcing arrangement occurs, one point remains the same - new data distribution points means increased risk and exposure for companies and their customers until they are reassessed.

On the surface the BPO outsourcing appears as a reduction in the cost associated with the outsourcing partner. From an information security perspective, red flags should pop up early, especially in the review process, to question the cost savings and how it will be achieved in light of potential increases in due diligence and due care. Information security brings enormous value to the table since part of our mantra is to ensure that businesses can truly keep those cost savings it expects while maintaining the proper security posture.

There will be many challenges ahead for information security professionals in the investigating, identifying and mitigating outsourcing to China. One challenge will require more in-depth analysis of the outsourcing company's business practices, methods, policies and even gaining insight into the contracts that managed their third party. In some cases, the arrangement is buried under layers of legal entities and companies incorporating in countries that pool the labor force in China. Another challenge will be determining and implementing the increased audit requirements necessary to comply with your regulations and information security best practices. This is the "hidden" cost associated with maintaining appropriate security levels for your organization, especially since there is an increase in the distribution of your business process data. To stay one step ahead of the trend, here are some key areas that can implemented to assist your business in managing the risk associated with government sponsorship, censorship and implementation of security controls:

Communicate Expectations: China is a new player in the world information security space. The same amount of attention we shared with India will be required with China in order to weave the fundamental information security policies and requirements in to fabric of its government and business law.

Research Chinese Business Laws: work closely with your legal team to determine the Chinese requirements placed upon your outsourcer. The findings should translate into service levels and capabilities in your new/ existing contracts.

Establish Due Diligence Depth: work closely with your legal, compliance and outsourcing team to build the appropriate depth to your due diligence analysis.

Understand Government Monitoring: China monitors and filters content to and from its population. The monitoring of encrypted traffic, such VPN, secure web transactions and file transfer should be identified to make sure that the outsourcers contractual commitments align with your expectations.

Explore Government Encryption Keys Access: China business laws may require access to encryption keys used to send and receive data to other countries. Determine how this access will occur and its implications on your existing key policies and procedures.

Investigate Security Breach Notification: inquire about the security breach process with issues that may emerge from inside China's borders. If a physical or technical breach occurs, you will need to determine if government censorship will prevent or filter disclosure. This can impact you ability to remain compliant with regulations in other countries.

Develop Sourcing Awareness: provide your sourcing team with the information necessary to design your outsourcing contracts so that they align with your industry requirements appropriately. This can also provide them the tools necessary to identify an information security caution flag which will allow you to engage early in the contract process to assist in building security-aware agreements.

If this trend in outsourcing continues there will be many new categories showing up in your transitional risk analysis, such as censorship, government laws, and restrictions. Getting ahead of these items and building a scalable process to handle them will bring efficiencies to your assessment process.

Rick Lawhorn (CISSP, CISA, CHSS, CHP, TCNP) is a Principle of Information Security & Compliance at Dataline, Inc. He has served as CISO at GE Financial Assurance & Genworth Financial and has over 16 years of experience in information technology. He can be reached at rick.lawhorn@mac.com or find him on the LinkedIn network.

Events around the world

Secure Denmark 2007
9 October 2007 – Copenhagen, Denmark
http://securedenmark.com

Smart Card Alliance Annual Conference 2007
9 October-11 October 2007 – Marriott Long Wharf, Boston, MA
http://www.smartcardalliance.org

Biometrics 2007 Conference & Exhibition
17 October-19 October 2007 – Westminster, London
http://www.biometrics.elsevier.com

Hack.Lu 2007
18 October-20 October 2007 – Kirchberg, Luxembourg
http://hack.lu

2007 Metro Louisville Information Security Conference
18 October 2007 – Churchill Downs in Louisville, KY, USA
http://www.regonline.com/issa-kentuckiana

RSA Conference Europe 2007
22 October-24 October 2007 – Excel London, United Kingdom
http://www.rsaconference.com/2007/Europe

3rd Annual Techno Forensics Conference
29 October-31 October 2007 – NIST Headquarters, Gaithersburg
Maryland
http://www.Techno2007.com

A multi layered approach to prevent data leakage

By Ulf Mattsson

Skilled malicious hackers are no longer interested in getting millions of people to open up e-mailed attachments that will then pester everyone listed in an infected machine's e-mail address book. Instead these people are becoming more business-like, concentrating on opening new streams of revenue for themselves by directly targeting and penetrating networks to grab data that they can use, or sell for profit.

Databases hold much of the most sensitive and valuable data – information about customers, transactions, financial performance numbers and human resource data to give a few examples. Despite this, databases remain one of the least protected areas in the enterprise. While perimeter and network security measures create a barrier against some type of attacks, there are attack patterns that take advantage of database-specific vulnerabilities.

An open invitation to breach the database

Since database management systems are complex, supporting an ever growing set of requirements and platforms, with addition of features they develop gaps in security – vulnerabilities – that are constantly being discovered by users, ethical hackers and unfortunately, non-ethical hackers as well. Such vulnerabilities are reported to DBMS vendors who do their best to patch them, but this is a process that currently takes several months on average, and in some cases years. That time lag is essentially an open invitation to exploit the vulnerability and breach the database.

The scenario reminds me of Willie Sutton, the bank robber. He answered the question why he robbed banks with –that's where the money is. He did not use the approach to stand at street corners to grab money from people passing by.

A widely used approach with current ATM systems is limiting the amount that you are allowed to withdraw in each transaction and for each day.

A layered approach to prevent data leakage

A layered approach can be very powerful in preventing data leakage. This approach should start with strong protection at the source, locking down sensitive information in critical databases. This should be combined with a monitoring and blocking capability, at the database query level, that can prevent all internal and external users, including database administrators from accessing data beyond the limit defined in their respective profiles. An enterprise solution should be able to monitor and block the data access volumes and transaction volumes at the application layer, database layer and file system layer. A comprehensive solution should also be able to dynamically escalate threat warnings across the applications, databases and file systems that are part of the data-flow for sensitive information. These different components can then respond with deeper analysis and activate a more restrictive policy for each access request that is targeting sensitive data.

It is usually fairly easy to find and lock down all major databases that store sensitive information like credit card numbers and customer information. This is an important first step since many information leaks – even those that eventually occur via stolen laptops or e-mailing sensitive information – typically originate with queries to critical databases with sensitive information. This approach can effectively limit the amount of sensitive data that is leaking out from sensitive central data stores to various distributed data stores.

A LAYERED APPROACH CAN BE VERY POWERFUL IN PREVENTING DATA LEAKAGE.

New patterns of attack

Just as there are new attackers, there are new patterns of attack. External hacking, accidental exposure, lost or stolen backup tapes, and lost or stolen computers are still significant sources of data leakage. But database attacks are often launched with the active participation of authorized insiders who extract critical data by abusing privileges, hacking application servers and SQL injections. Even well-protected databases may offer applications broad access privileges, beyond those granted to any individual. Access through an application may effectively circumvent infrastructure-based defenses. So-called “home-user” attacks inject SQL commands into otherwise innocuous fields, compromising database security from outside corporate networks. Among the most dangerous avenues of attack, this is also one of the oldest: a trusted but untrustworthy employee applying broad access privileges. Many organizations have formal access policies and processes that govern how and when sensitive data is accessed, but lack practical and cost-effective solutions for detecting or blocking activities that fall outside these policies.

Database attacks are often launched through insiders

Database breaches—often attacks by organized criminals working through authorized insiders—target valuable concentrations of business-critical information. Business impacts are immediate and profound, and damage to company and personal reputations can last for years. Database breaches are a growing component of IT Risk.

There is growing recognition that the “insider threat”, and specifically the threat posed by users with privileged access, is responsible for a large number of data breaches. According to annual research conducted by CERT, up to 50% of breaches are attributed to internal users. The 2006 FBI/CSI report on the insider threat notes that two thirds of surveyed organizations (both commercial and government) reported losses caused by internal breaches, and some attributed as much as 80% of the damage to internal breaches. It was also reported that 57% of implicated insiders had privileged access to data at the time of breach. It is therefore evident that perimeter and network security measures are not enough to stop such breaches.

Driven by the consolidation of valuable information and the professionalization of computer crime, database attacks are often launched through insiders with full authorization to access the information they steal. Both the Computer Security Institute and the FBI survey document the rising incidence of such attacks. Infrastructure security solutions such as perimeter-based defenses, access controls, and intrusion detection can do little against authorized insiders. And the fact remains that no screening and authorization process can be perfect.

Unauthorized behaviors by authorized and unauthorized users

Database attacks represent unauthorized behaviors, by both authorized and unauthorized users. As we have seen, authorized insiders constitute a major threat against information safety and integrity. Barring a perfect screening process, no permission-based, asset-centric security system can close this fundamental vulnerability.

The problem grows worse

Business enterprises and security companies are in the early stages of their response to the resurgence of threats to their information assets. Yet as they struggle toward solutions, the problem grows worse. More information is made available to customers, partners, and suppliers through Web portals, often linked to critical databases. Companies integrate customer-facing applications such as customer relationship management, service provisioning, and billing more tightly, spreading critical information more widely within and across organizations. In addition more businesses outsource and offshore critical business processes to new “insiders” who may not meet their own organizations’ internal screening processes. Increasingly automated management of intellectual property, for example in pharmaceutical companies and genetic research, may put corporate assets of significant value in highly-accessible databases Virtually any organization, public or private, is at risk of public embarrassment, financial loss, and government investigation when critical information is stolen or compromised.

More complexity - more issues

Attack an application often enough and you’re bound to find exploitable holes. Databases complicate the issue by being complex beasts that feed information to and from other applications – some vendor-supplied and others perhaps created in-house or via supplied APIs. The more complex an application becomes, the more likely it is to harbor hidden holes.

New Security Requirements

Security is shifting from protecting the device and learning about individual users to thinking about the policies that I deploy around user interactions and information protection, and having policy management techniques and technologies that give me warnings or block access or activity when it doesn’t conform to what I had prescribed.

Organizations will need multi-layered ways to defend their sensitive information

As the Web has become a ubiquitous operating tool, the risks to businesses have multiplied. If online infrastructures are not protected and have unsecured entry points, companies both large and small are putting their networks at risk. While firewalls are common in every organization, they are no longer sufficient to ward off hackers intent on stealing confidential information. Organizations now realize that they need to have a solid online security policy in place to assure consumers and trading partners that their information is safe.

Blocking based on the volume of data accessed

The defining security requirement for Data-layer security is the ability to detect out-of-policy data access by outsiders or even authorized insiders, through direct access to the database itself, or over networks including the Web. Alerts and blocking based on comparisons with historical patterns of usage, provides continuous, actionable exception monitoring of transactions that may contain protected data. Solutions must monitor and block out-of-policy transmission of typical patterns such as credit card numbers, Social

Security numbers, patient record identifiers and other patterns as defined by enterprise administration.

Limitations of traditional approaches

There is a wide array of technologies currently in use for securing databases. As with other areas of IT security, no single tool can provide ironclad defense against all threats and abuses. It is always recommended to employ a combination of tools to achieve adequate security. Traditional perimeter and asset-based defenses won't work effectively in environment in which perimeters are indistinct and constantly changing, where attacks are marshaled against data, not assets, and where the most likely threats are from fully-authorized insiders with the capacity to circumvent or neutralize defenses.

Perimeter-based defenses offer little protection for critical information

Perimeter-based defenses such as firewalls and intrusion-detection systems are the bedrock of IT security and more necessary than ever, but they offer little protection for critical information stored in databases. First, they are ineffective against attacks by insiders with full authorization to operate inside defended perimeters. When the organization's trust in its authorized personnel is justified, perimeters are unlikely to provide the same degree of protection as in the past. With the security perils of mobile systems, wireless networks and peer-to-peer "sharing" networks, high-capacity USB "thumb" drives, portable hard drives, and other mobile storage devices, with an array of mechanisms to move information across networks without detection, perimeter defenses can do little.

ROLE-BASED RATHER THAN BEHAVIOR-BASED, ACCESS CONTROLS AND PERMISSIONS ARE DIFFICULT TO DESIGN AND MAINTAIN.

Identity Management and Access controls are difficult to design and maintain

Unfortunately, it is very common within enterprises to have group usernames and passwords and to forget to revoke privileges of employees who no longer need them. This mechanism is also exposed to hacking (e.g., SQL injections that escalate privileges). Role-based rather than behavior-based, access controls and permissions are difficult to design and maintain. Among other problems, "permission inflation" gradually weakens protections over time as individuals acquire new permissions when their job roles change. Access controls also seldom apply to access through applications, for example through SQL injection.

Monitoring using Network Appliances

Monitoring using Network Appliances can provide alerts (and if used in-line, prevention) on network access to the database, but do not protect against insiders with access privileges / local access. They often require network reconfiguration, and if used in-line slowly create a network bottleneck that cannot handle encrypted traffic or expensive hardware.

This is a class of network-based appliances, which monitor network traffic looking for SQL statements, and analyze the statements based on policy rules to create alerts on illegitimate access to the database and attacks. Because the appliance is only monitoring the network it does not have visibility into local database activity, essentially leaving the database vulnerable to insiders that either have local access or are savvy enough to bypass the appliances. In order to provide adequate monitoring, the appliance must be deployed at every choke point on the network where the database is accessed, encircling the database from all sides. For mission-critical databases that are often tied into a multitude of applications (ERP, CRM, BI, billing etc.), this significantly raises the cost, which is high to begin with.

Slow and imperfect protection with intrusion detection and Audit

Intrusion detection on database servers can't resolve authorized from unauthorized queries.

On networks, intrusion detection protects only information in transit from very narrow types of attack. While absolutely necessary for an effective IT policy or regulatory compliance program, audits tend to be resource-intensive, consuming a great deal of time and effort and cutting into system performance while underway. And unless audit data is accurate and mapped clearly to data instead of infrastructure, and itself protected from attack, audits offer slow, imperfect protection against internal attack.

Unfortunately, neither perimeter defenses, employee screening, nor information-focused security can prevent accidents—as when a laptop containing credit card numbers is misplaced. Only information-centric security can help managers and auditors understand what information was lost in order to guide notification and remediation efforts.

Native database audit tools

Native Database Audit Tools provide a granular audit trail and forensics of database activity, but come with a serious database performance impact. They offer only after-the-fact forensics and have no prevention capabilities, no separation of duties and are easy to turn off. Most DBMSs come with a set of features that enable granular auditing of every single database activity. These features are seldom used because of the negative impact they have on performance. Furthermore, because they are part of the DBMS, they are administered by DBAs in a way akin to “letting the cat guard the cream”.

Data encryption adds an essential level of protection

Database activity monitoring cannot provide protection against privileged insiders or malicious users, but policy driven encryption of database fields can offer good protection of information. Encryption systems should be controlled by a separated policy and also linked to a multi-layer protection approach. Data encryption adds an essential level of protection from intruders who manage to break through primary defenses, and also ensures data is seen on a need-only basis as determined by access permissions protecting it from exposure to authorized and unauthorized users. Encryption is a necessity in all situations in which customers can perform (or authorized users are provided access to) transactions involving confidential information stored in a database. Any decent security program must ensure that secure automated encryption management - including secure encryption key protection, aging, and replacement - is implemented across all platforms hosting critical information. The best cryptographic architecture will be flexible and modular so that it can be easily adapted to various situations across the enterprise. The challenge, as always, is to find the right balance between security and usability. There is no one perfect architecture for all companies, as business policies and associated compliance issues will determine what data needs to be protected and what methods to use. The important thing is to be willing to go beyond compliance basics and develop a workable and comprehensive plan to secure data that suits the needs of your company.

Solutions for Multi-tiered applications

Privileged access to critical databases

Asset-centric approaches to database security can actually increase risk by wasting time, effort, and focus on solutions unlikely to slow information loss and corruption. Innovations such as multi-level applications, multi-tier storage, and service-oriented architectures (SOA)—often with privileged access to critical databases—raise the complexity and vulnerability of critical data structures. In any of these environments, the mapping of information onto infrastructure assets is complex, and changes constantly. Asset-focused policies, alerts, security logs, and reports are complex and interdependent, and may even be irrelevant for protecting data, and documenting compliance to data-focused policies and regulations.

Who is the real user?

Current data security systems for data at rest, whether they are implemented as separate server appliances, co-located with one or more applications on the same host machine, or co-located with data services machines such as database servers, operate in real-time, intrusively in-line with the data they protect. When sensitive, encrypted data is requested by applications rather than directly by authenticated users, the "legitimate user" is frequently no more than the application name itself. Even in cases where an actual username is passed from the application along with the data request, the data security system is "blind" to whether or not the user is a hacker or has stolen legitimate user credentials.

A behavioral policy can restrict access even if the real user is not identified

Data security systems are not configured to take advantage of application security events detected elsewhere in the environment in the same approximate timeframe. Although correlation with those events is a typical practice when auditing the forensics of events via log files, long after the events have occurred.

Some approaches track who the real application user is based on a probability analysis across concurrent processes that are accessing the data. Other solutions can completely track the user but these solutions are application aware – either based on an application API or a plug-in that is specific to each application environment. The behavioral policies restricting access to data are analyzing access patterns and does not require that the real end user is identified.

DATA SECURITY SYSTEMS ARE NOT CONFIGURED TO TAKE ADVANTAGE OF APPLICATION SECURITY EVENTS DETECTED ELSEWHERE IN THE ENVIRONMENT IN THE SAME APPROXIMATE TIMEFRAME

Solutions for Web based applications

Buffer overflows, SQL injection and Cross Site Scripting

Buffer overflows and SQL injection aren’t new, but attackers still manage to make effective use of them to gain access and administrative privileges to databases. Intrusion prevention systems are of use in dealing with buffer overflows. SQL injection is a popular method of attack, since modern databases utilize SQL - Structured Query Language - to enable users to access and manipulate data stored in a database. The basic procedure for a SQL injection exploit is to provide a valid request at the beginning followed by a single quote and a “;” with an additional request appended which contains the actual command the attacker hopes to implement. By piggybacking the “bad” code onto the good code it’s possible to trick an incorrectly configured database into carrying out unauthorized executions. Cross site scripting occurs when a web application gathers malicious data from a user. The data is usually gathered in the form of a hyperlink which contains malicious content within it. The user will most likely click on this link from another website, instant message, or simply just reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in HEX (or other encoding methods) so the request is less suspicious looking to the user when clicked on. After the data is collected by the web application, it creates an output page for the user containing the malicious data that was originally sent to it, but in a manner to make it appear as valid content from the website.

Latency issues with traditional application firewalls

Web application firewalls are often the easiest way to protect against these sorts of exploits. Code audits in-house, or by an outside expert can also spot and close SQL vulnerabilities. Most application firewalls, whether they are implemented as separate reverse-proxy server machines, co-located with the application on the same host machine, or co-located with network firewall machines, generally operate in real-time, intrusively in-line with the applications they protect. This introduces latency while the application firewall examines the traffic, logs the activity, alerts IT Operations and/or network firewalls to suspected attacks and passes traffic on to the application. Additional latency is introduced when HTTPS traffic is examined. For instance, secure socket layer ("SSL") protocols used in HTTPS are terminated and decrypted prior to examination; in some implementations, traffic is additionally encrypted again before passing traffic on to the Web, application, and/or database servers for final HTTPS termination. Application firewalls are not configured to take advantage of security events or behavioral anomalies detected elsewhere in the environment in the same approximate timeframe, although correlation with those events is a typical practice when auditing the forensics of events via log files, long after the events have occurred.

Web application firewalls combined with an escalation system

Automated, synchronized threat monitoring and response between the application level and database level provides a highly effective protection against both external and internal attacks. An escalation system that can dynamically switch Web application firewalls between different protection modes is described below.

Behavioral policy layers can restrict data access

Control database queries that returns thousands of credit card numbers

Unlike monitoring tools that only inspect inbound database commands; this approach identifies unauthorized or suspicious actions by monitoring traffic both to and from database servers. This allows the solution, for example, to immediately identify a database query that returns thousands of credit card numbers, thereby deviating from data access patterns.

How to understand the true extent of data theft

A Policy Engine that monitors outbound responses from the database can detect suspicious data access patterns, based on volume of returned records. Data Usage Policies are typically used to detect activities by authorized users that fall outside normal business processes. Information collected by the Data Usage Policy Engine can also be used to understand the true extent of data theft, thus minimizing breach disclosure efforts and costs. A solution may provide access and security exception policies that monitor inbound database commands for unauthorized actions, such as database changes, failed logins, and SELECT operations by privileged users.

Control the amount of data that is accessed

Protection rules control the amount of data that is allowed for each user to be accessed in certain time windows. The item access rates define the number of database records, file blocks or web transactions that is allowed for each connection in a time window. The item access rates can be defined based on the number of rows a user may access from a database column. For example if a query result exceeds the item access rates, the request is blocked before the result is transmitted to the user.

Prevent the result of the query to be accessed by the user

The method for detecting intrusion in a database can be based on an intrusion detection profile, with a set of item access rates, which includes a definitive number of rows that may be accessed in a predetermined period of time for each user. When a query is exceeding an item access rate defined in the profile user authorization the result of the query is prevented from being transmitted to the user.

Data inference policy rules

A variation of conventional intrusion detection is detection of specific patterns of information access known as inference detection. Inference detection is deemed to signify that an intrusion is taking place, even though the user is authorized to access the information. Results from performed queries are accumulated in a record, which is compared to the inference pattern in order to determine whether a combination of accesses in said record match the inference policy, and in that case the access control system is notified to alter the user authorization, thereby making the received request an unauthorized request.

Machine-learning from accepted patterns and past intrusions

The behavioral policies restricting access to data can utilize machine-learning from accepted behavioral patterns and from previous intrusions in order to better predict future intrusions.

A Multi-layered Data Defense system

A layered approach to security

No single approach to securing a system will be able to defeat each and every new and innovative intrusion attempt by insiders and/or outsiders. That's why we deploy layers of protection. If one or two fail another will withstand the attack, or at least slow down the criminal who is likely to give up and ransack a more vulnerable target. Many crimes, including network attacks, are crimes of opportunity and the easy way in and easy way out becomes the thief's preferred modus operandi.

Data-layer protection

A Data-layer protection approach monitors all requests for sensitive data access for critical data such as credit card and Social Security numbers, patient identifiers or custom patterns. Comparisons against policy and history identify exceptions and anomalies in real time, and provide a comprehensive audit trail to document compliance. Any genuine long-term solution must be flexible and include options to balance protection level against database performance and other operational needs.

A multi-layer security advisory framework

A Multi-layer Security Advisory System provides a framework to effectively deal with threats of some classes of attacks. The warning system has 5 risk-of-attack-levels (Threat Levels) which when triggered, initiate specific actions by local servers within the same policy domain. Information about data security events is collected from sensors at different system layers (web, application, database and file system). The Threat Level is propagated to systems that are connected within a data flow. The Threat Level will also adjust for time of day, day of week, and other factors that are relevant.

A score-card to keep track of usage abnormalities

A score-card is maintained for each subject (user or service account/proxy-user, IP address, application, process) and object (database column, file) with a history of processing sensitive data. The score-card summarizes current and historical information about data access patterns for each entity (subjects and users). The score-card also includes a 'fingerprint' that reflects historical deviation from acceptable access patterns at the level of s/i/u/d (select/insert/update/delete) operations. A high score-card value will initiate more extensive analysis before releasing data to the subject. The dynamic and automatic altering of the protection policy between multiple system layers includes modifying the protection policy of data at one or several of the system layers. The modification is performed based on a result of the prevention analysis. The score-card can also keep track of when a remote system need to reconnect to the central system to renew or recharge it's capability to encrypt and decrypt data. The policy may allow the local system to only operate stand alone for a certain time or processing a fixed number of crypto operations between each host connection and central password renewal. This behavior will act like a rechargeable key box and can automatically shut down the local access to sensitive data in case the local system is stolen, cloned or compromised in some other way.

Escalation in a multi-node security system

This is a method for achieving cooperative processing and control of application-layer security by using loosely and tightly coupled nodes of application firewalls, application monitors and data security enforcement points together with operational and escalation rules. For example a SQL Injection attack at the application layer can automatically switch the Web Application Firewall from monitoring mode to inline mode to block certain requests. This will provide a dynamic and automatic altering of the protection policy.

Escalation in a mufti-layer security system

The dynamic and automatic altering of the protection policy between multiple system layers includes modifying the protection policy of data at one or several of the system layers. The modification is performed based on a result of the link prevention analysis. For example a SQL Injection attack at the application layer can automatically put the connected backend databases in a higher alert-level (System Threat Level). The higher alert-level can switch to a protection policy that may turn on additional logging and alerting and potentially also block certain requests when the score-card is out of balance.

Balance performance and protection

In meeting the requirements above, Data-layer protection must be flexible to adapt to different requirements related to protection level, performance, scalability and other operational needs. A multi-layer solution can balance performance against the level of protection against internal threats, and can minimize required modifications to the database or associated programs.

The Multi Layered Database Security approach to data security provides policy-driven, data protection in real time with customizable balancing between zero performance impact and full protection against internal threat against data at rest.

Selective activation of the intrusion analysis

Access to selected data columns or files can trigger a deeper intrusion analysis process. This is especially advantageous if only a few items are intrusion sensitive, in which case most queries are not directed to such items. The selective activation of the intrusion detection will then save time and processor power.

Dynamically switch between monitor and in-line operation

The Leakage Prevention solution can dynamically block the transaction output results that violate security policies. This can be accomplished by dynamically switching the solution between in-line database gateway operation and operating as a passive monitoring device that initiates other enforcement actions such as transaction blocking, automated logouts of database users, VPN port shutdowns, and real-time alerts.

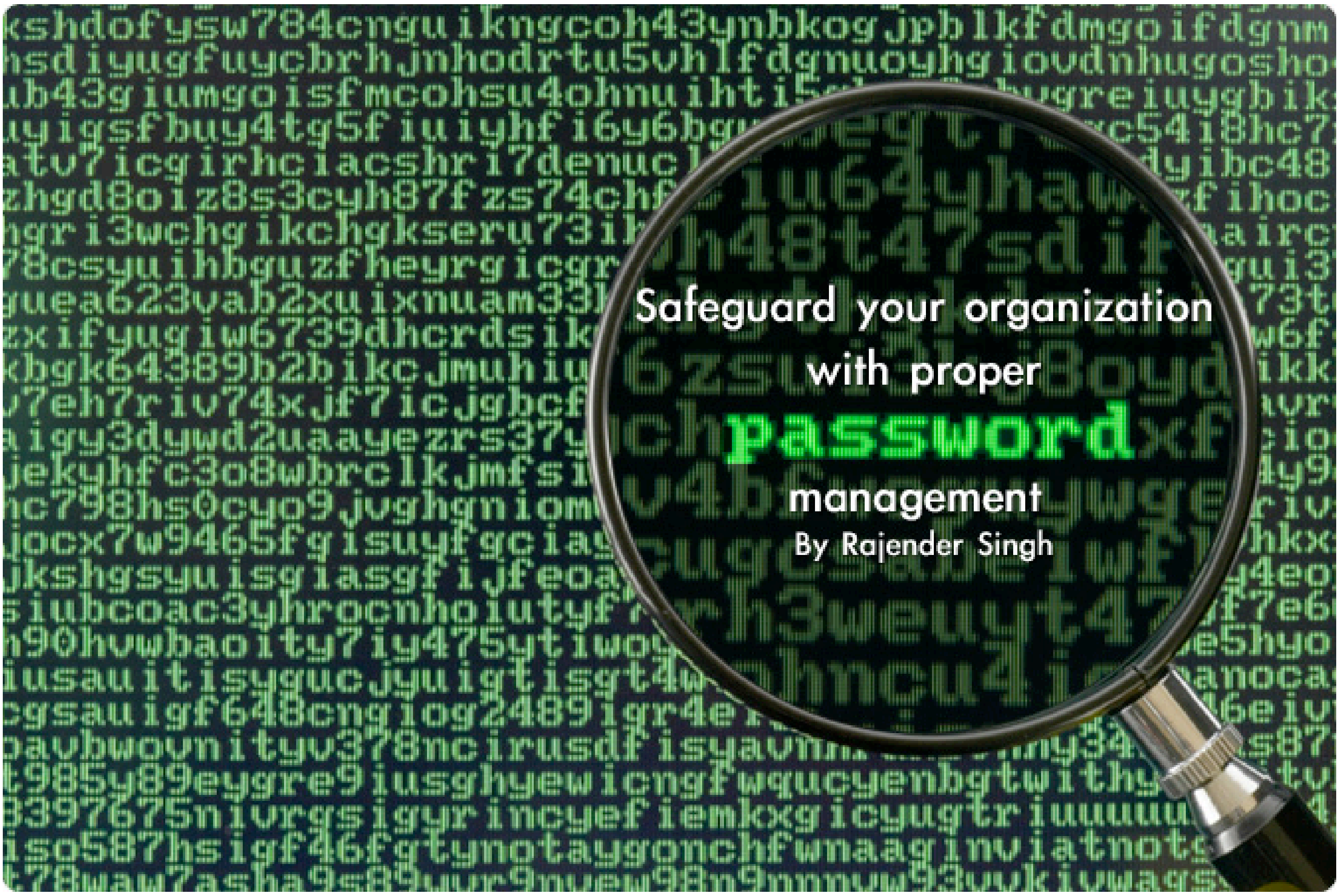
Conclusion

The proposed Multi Layered Approach to prevent Data Leakage meets many fundamental requirements of organizations to protect their critical data from loss, leakage, and data fraud. Data leakage can be minimized by real-time detection and blocking of leakage of sensitive company information—including analysis of all sensitive data leaving the database, so companies can react immediately to policy violations. Fraud from insiders abusing privileges can be minimized from analysis of behavior against established policies and access history to identify anomalous behavior, even by authorized users, so that organizations can achieve “defense in depth” for all sensitive data under their care.

The approach can provide protection against poorly-written applications that open vulnerabilities to critical databases and files. The approach can also provide an alternative to some of the frequent patching of critical systems.

In addition to dynamically providing minimal and adjustable performance impact, this approach can offer flexibility and dynamic features that can switch to use selected security features when an escalation is needed. To assure timely response, solutions should provide real-time tracking and blocking, not relying solely on alerts or reports after the fact. In addition, audit data should be archived off of the server holding the data, so that the audits themselves are not vulnerable even in the event of a database breach.

Ulf T. Mattsson is the CTO of Protegrity. Ulf created the initial architecture of Protegrity’s database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization, in the areas of IT Architecture and IT Security. Ulf holds a degree in electrical engineering from Polhem University, a degree in Finance from University of Stockholm and a master's degree in physics from Chalmers University of Technology.



Safeguard your organization with proper password management

By Rajender Singh

Access control is one way to ensure security in your organization. An intruder can break into your network by compromising accounts with weak passwords. If the compromised account turns out to be a privileged account, or if the intruder escalates privileges, then you may be looking at catastrophic damage to your organization's IT systems.

The first step to prevent such attacks is to ensure your organization's security policies and procedures incorporate strong and comprehensive account and password management processes. A password undergoes certain states of existence, with owners for each state, who are involved in handling those states. These are:

Different states of a password	
State	**Owner**
Account creation	Change management body
Password selection or Changing default password	User
Change password after nth day	User
Auto password expiry	System
Auditing Systems for weak password	Auditors / Tools / System admin / Security manager

The different stages in password management are: creation, administration and review / auditing.

Here are the recommended best practices to ensure comprehensive password management.

Using a Strong Password

A password must be *strong enough* so that it cannot be easily breached by brute-force or dictionary attacks. The selection of a strong password involves criteria such as the usage of alpha-numeric character sets along with upper and lower case alphabets and the use of special characters. On the other hand, insisting on highly complex passwords may well result in users having problems with remembering these passwords.

Ensure your IT security team and security managers make users aware of the reason behind strong and complex passwords and teach users ways of remembering complex passwords. Functionally, we can surmise the complexity of a password is a function of the length of password and number of character sets available to create that password.

Password complexity = f (length, character set).

Password Expiry

Even with a complex password, you could still be at risk. Today's clustered computing environment could well break your password in a few days or weeks at the most. It is always recommended to change your password after a certain number of days. If you change passwords at a frequency of 30 days and if an intruder works on your password hash and is able to crack it in 45 days, you are still secure as you have changed your password to another strong password, ahead of the intruder.

Limit number of login attempts

At any point of time, an account could undergo password cracking attacks. In such attacks, the attacker uses scripts or tools and tries to use brute-force or dictionary attacks against specific or some users. To guard against such attacks, the authentication system must limit the user to a certain number of (failed) login attempts, after which the account should be locked out. The disadvantage of this approach would be a genuine user not being able to login if somebody is really trying to break into his account.

Remember historical passwords

Users have a tendency to repeat their passwords in many accounts and repeat it while being prompted to change passwords. As explained, the downside of keeping the same password for a long time can lead to the compromise of the user account. It is recommended that your IT security setup should prevent users from keeping the same passwords for at least 3 to 5 password resetting operations.

Show last successful login

One way to create transparency among the users regarding their account would be to give them details of when they last logged into the system or network. This would help them analyze their own account. At least 3 previously successful logins must be displayed with time, date and duration of login. If a user suspects the account has been misused by somebody, the user should log a security incident with the IT security team, and the IT security team should audit this breach.

Store passwords in encrypted form

If passwords are stored on the local disk or transferred over a network, they must be under secure communication channels. This would offer protection against password sniffing and cracking attacks.

Enable ticketing system for password resets

Today, many organizations manage password reset requests via ticketing systems. In a ticketing system, after getting authenticated, user should be in a position to log a ticket for password resets.

Authentication is very important while filing such requests, to ensure that a malicious user cannot set up a reset request for an unauthorized account. Such tickets must be logged for further analysis and reference.

Practice password auditing

Automated tools or open source password crackers can be very useful in auditing passwords. An organization will face a major security risk if the accounts of senior associates or critical users have been compromised. Performing password audits will provide clarity on the efficiency of the password management policies.

Reporting and closure reports

Providing reports on weak passwords, password resets and change of password to users along with security managers is very useful. Reports have always added value in showing the existence of such incidents and tracking them to closure in order to make organization more secure and ready for audits.

Security awareness

Even with the best set of policies, there's always a chance that passwords can be compromised. Sharing passwords with others, writing down complex passwords on a Post-It, social engineering and man-in-the-middle attacks are just some of the 'password harvesting' techniques.

Sadly though, these issues are ignored by users and will lead to compromise of these strong passwords. It is important that users be aware of such techniques, therefore your IT security team should conduct regular user awareness sessions and include possible attacks and attack scenarios in order to make everyone aware of common pitfalls.

Conclusion

We have discussed various parameters which should be part of your security procedures and password policy to strengthen your organization's IT security. To derive the value of these best practices, visibility and awareness among all users along with implementation of such practices on systems is required.

Rajender Singh is an IT security consultant with experience in deploying BS7799/ISO27001 based information security management system. He is a pen-tester and avid sailor. Rajender assists clients in implementing robust IT security procedures.

Security blogs spotlight

Network Security Blog (www.mckeay.net)

Martin McKeay has been offering quality insight into current security issues since 2003 which makes him one of the most prolific security bloggers and podcasters. If you visited some of the popular security conferences in the US this year, you probably saw him making informative videos for PodTech.

TaoSecurity (taosecurity.blogspot.com)

A legend among security bloggers, book author and network security expert Richard Bejtlich writes about incident response, network forensics, security monitoring and FreeBSD. He's also an avid reader of technical material and publishes many book reviews which can help you decide on your reading list.

Jeremiah Grossman (jeremiahgrossman.blogspot.com)

Web application security guru, CTO of WhiteHat Security and co-author of “XSS Exploits” Jeremiah Grossman, runs an outstanding blog that uncovers a myriad of useful information about web application security.

Mind Streams of Information Security Knowledge (ddanchev.blogspot.com)

Dancho Danchev's blog covers topics related to information warfare, malicious tools, malware, spam, phishing, and a variety of other topics. If you’re looking for detailed analysis of current threats this is a blog to keep an eye on.

Interview with Ulf Mattsson, Protegrity CTO

By Ericka Chickowski

Ulf created the initial architecture of Protegrity's database security technology, for which the company owns several key patents. His extensive IT and security industry experience includes 20 years with IBM as a manager of software development and a consulting resource to IBM's Research and Development organization, in the areas of IT Architecture and IT Security.

Let's end the debate: Are hardware-based tools or software-based tools the best way to encrypt and decrypt databases?

I think that might be the wrong question to ask. The right question would be about the topology. What is the right topology to use for database encryption? Remote encryption or local encryption?

The topology is crucial. It will dictate performance, scalability, availability, and other very important factors.

I think the topic is important but the question is usually not well understood. Usually, hardware-based encryption is remote and software-based encryption is local but it doesn't have anything to do with the form factor itself. Instead, it is about where the encryption is happening relative to your servers processing the database information.

Why do you think people are asking the wrong question?

It is because they are trying to apply what they've learned from other areas of IT. For example, from network encryption they've seen that software doesn't perform as well and that hardware is the best way to accelerate encryption. So they say, "Oh, hardware is the answer, that's the way to offload processing requirements." And they jump to the conclusion that this must be true for database encryption as well.

Why don't these principles apply to database encryption?

When you have, say, credit card data, you have to remember that databases usually operate on the field level. You cannot send more data than one credit card number at a time.

You encrypt it and then you need to give it back to the database immediately because it is sitting there waiting to send the next one. This is particularly a problem with decryption. For example, when someone is searching data and can't wait for slow response times.

When you compare this process between local and remote encryption, the path length—the number of instructions that the computer needs to satisfy your request—is so much longer when you send the data over some kind of network and then receive it back compared to just doing it locally. It could be up to a thousand times longer of a path length to send it to a remote appliance compared to doing the decryption locally on your data server.

Sometimes it is important; in other cases it doesn't really matter.

How do you determine if it is important to your enterprise?

First, you need to determine whether you are doing batch or online processing. If it is batch processing you'll need to determine what kind. Are you doing more normal batches where you have a batch job that must run in four hours, or a sequence of batch jobs that need to be finished before morning? Or are you interested in data loading where you can take a chunk of data and go off and process the data and come back and no one is missing it in the meantime? If you're doing online transactions then you'll need to determine if it is online transaction processing with transactions that you're processing one record at a time while the user is sitting there waiting, or if you are doing online data warehousing where you're searching large amounts of data at once.

DATA LOADING IS THE GRAY AREA WHEN IT COMES TO LOCAL OR REMOTE ENCRYPTION

Let's tackle batch processing first. How will the topology affect encryption activities during this type of processing?

If it is a normal batch, I'm sending it over the wire and my database is sitting there and waiting for every credit card number to be encrypted and come back before sending another one and continuing the cycle. If I send it to a remote platform, the batch will stop and wait maybe a thousand times more than I'd expect. Therefore, a batch job that would normally take eight hours might take eighty hours. That's not overnight—it isn't even over two nights!

Then we have data loading. Sometimes it can be nice to encrypt the data on a cheaper platform before you load the data into your production database. So you pre-encrypt it, offload it and do it with cheaper equipment. That's provided you have the time.
But if you are, for example, in a retail environment you might have a time constraint. You need to load the data from your four thousand stores in a certain window. And at that point you may want to use all of the processing power that you have invested in to get the data loaded. That means that you still want to do the encryption locally in your big database server to take advantage of that high end system.

Data loading is the gray area when it comes to local or remote encryption. It depends on whether you really want to offload the processing or if you want to do the data loading very quickly.

And what about online processing?

Both of the major use cases are detrimentally affected by remote encryption.

If I have a data warehouse and the user is sitting there and needs to search among 100 million records or maybe five billion records, like some of our credit card customers, then it's crucial how much time is consumed for each decryption. The person is sitting there waiting for hundreds or millions of records to be decrypted before the answer comes back.

If you do it locally, you may have a response time of around five micro-seconds for each record and then you multiply by 100 million if you have 100 million records and so on. Compare that five micro-seconds for local encryption to the case of remote encryption.

You may have a thousand times greater processing time, so if you add up that time the user may wait for an hour instead of one second.

In online transaction processing, one user may not see a difference between local and remote encryption. Because if one user is looking for one record in the database, the difference between five microseconds and five thousand microseconds is not noticeable. But if you have high volume of processing on your computer it will matter. If you add up all of your transactions and each of them takes a thousand times longer than necessary, you will hit the roof and you will overload your computer. It can really cripple you.

But what if I have a fast network? Won't the speed of the hardware appliances and the speed of the network mitigate the issues you've mentioned?

It is interesting also to notice that fast network doesn't really help you. If you summarize all the steps that need to be processed for the data to go all the way from the database, over to another appliance and back, that path length is so much higher that the network speed doesn't really help you.
Another thing to think about when you dissect this is, if you want to be secure, you actually need to encrypt the wire between the appliance and your database server. Guess what? It costs you more overhead to encrypt that traffic than to do the encryption in the first place.

Another myth is that the speed and the power of the appliance is going to affect the total speed of the encryption and decryption processing. The marketers will say, "Well, we can stack appliances so that you can harness this enormous power of these boxes. Put it on a fast network and you can really offload the processing."

Sounds good, right? On the surface it sounds nice but the truth is quite contrary to what they're saying.

I think it is important that everyone understands that this is not spin; this is what the industry has seen in benchmarks during the last 10 to 15 years. I usually cite figures in my papers and so far no one has come back to dispute them.

DEFCON 15

By Vlatko Košturjak

Defcon, the legendary hacker convention, this year celebrated its 15th anniversary. Defcon 15 took place at the Riviera in Las Vegas, 3rd to 5th August.

Registration at Defcon is very smooth and privacy oriented. You don't have to tell your name or leave any personal information. Just give up $100 and you'll get a badge, sticker, agenda and a Defcon CD.

The badge is definitively unique and it deserves few words in this text. It has batteries and electronics around it. By default, it can display custom messages on the included LEDs, Naturally, Defcon participants hacked it immediately and implemented various cool stuff including one time password (OTP) generators. The badge is definitively a proof of the creativity of the convention organization that stimulates the minds of the attending hackers.

On the first day of the convention, an unusual event took place and news about it soon covered the Internet. Convention attendees were warned about an undercover reporter. For those who don't know, Defcon has a strict policy against media and their filming conference attendees. Media must get permission from any individual that will be filmed (and sweeping the room with TV camera is forbidden). All journalists covering Defcon must sign such an agreement. Some of the journalists didn't take that seriously. Specifically, Dateline NBC associate producer Michelle Madigan. She registered as a regular attendee, in order to bypass the legal agreement. It is believed that NBC sent her with a hidden camera to the event to capture hackers admitting to crimes. She was soon led into a large auditorium and then organizers announced her presence and her intentions. She immediately started to flee. Of course, she was followed by dozen of reporters and conference attendees.

There are videos covering the incident and you can see them on YouTube.

The talks at Defcon were very up to date. Lectures covered security issues in every IT “buzzword” today, from SOA and Web 2.0 to RFID and virtualization. What I like at the Defcon is friendly and intelligent atmosphere at every lecture I attended. There were lots of famous security speakers including Bruce Schneier (popularly called the “Chuck Norris of Information Security”).

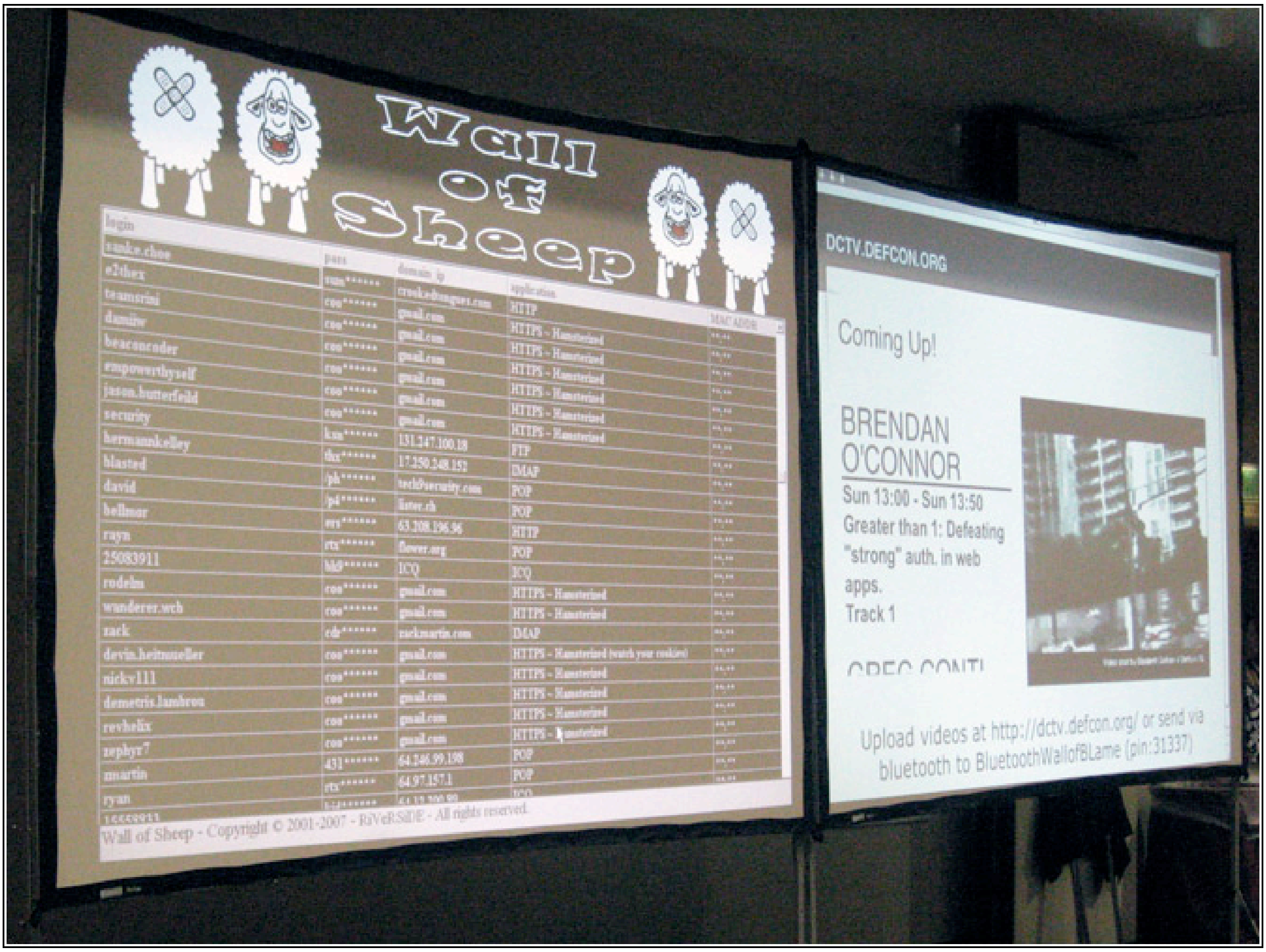
I'd like to point out to few interesting lectures. Let's start from the lowest level of the ISO/OSI layer :) Zac Franken demonstrated how you can hack a physical security access control reader. He focused his attack on the lack of reader installation security (i.e. protection of the cables that goes to the access control reader).

"Security by politics - why it will never work” was presented by Lukas Grunwald who talked how security by politics is bad idea by giving examples of the recent introduction of RFID passport systems.

"Breaking forensics software" was mostly about Encase potential vulnerabilities and how you can hide data from forensic teams who use Encase. I learned that you can use the 26th partition to hide data (Encase only recognizes only first 25 partitions), an issue that should be fixed in the next release of Encase.

I could go on and mention every lecture I attended, but it wouldn't be so interesting as attending yourself, which I definitively recommend you do next year.

Defcon has a large number of contests during the convention. The most famous is hacker's way of Capture the Flag game. There is also lock-picking contest, wireless contest, 0wn the box contest, and more.



login	pass	domain / ip	application	MAC ADDR
sanke.chee	sun******	crookedtongues.com	HTTP	**:**
e2thex	coo******	gmail.com	HTTPS - Hamsterized	**:**
teamsrini	coo******	gmail.com	HTTPS - Hamsterized	**:**
damiiw	coo******	gmail.com	HTTPS - Hamsterized	**:**
beaconcoder	coo******	gmail.com	HTTPS - Hamsterized	**:**
empowerthyself	coo******	gmail.com	HTTPS - Hamsterized	**:**
jason.butterfeild	coo******	gmail.com	HTTPS - Hamsterized	**:**
security	kun******	131.247.100.18	FTP	**:**
hermannkelley	thx******	17.250.248.152	IMAP	**:**
blasted	/ph******	tech@security.com	POP	**:**
david	/pd******	lister.ch	POP	**:**
bellmor	ers******	63.208.196.96	HTTP	**:**
rayn	rts******	flower.org	POP	**:**
25083911	hh0******	ICQ	ICQ	**:**
rodelm	coo******	gmail.com	HTTPS - Hamsterized	**:**
wanderer.web	coo******	gmail.com	HTTPS - Hamsterized	**:**
zack	cdr******	zackmartin.com	IMAP	**:**
devin.heitmueller	coo******	gmail.com	HTTPS - Hamsterized (watch your cookies)	**:**
nickv111	coo******	gmail.com	HTTPS - Hamsterized	**:**
demetris.lambrou	coo******	gmail.com	HTTPS - Hamsterized	**:**
revhelix	coo******	gmail.com	HTTPS - Hamsterized	**:**
zephyr7	coo******	gmail.com	HTTPS - Hamsterized	**:**
mmartin	431******	64.246.99.198	POP	**:**
ryan	rts******	64.97.157.1	POP	**:**
15555911	[illegible]	64.12.200.89	ICQ	

Wall of Sheep - Copyright © 2001-2007 - RiVeRSiDE - All rights reserved.

DCTV.DEFCON.ORG

Coming Up!

BRENDAN O'CONNOR

Sun 13:00 - Sun 13:50

Greater than 1: Defeating "strong" auth. in web apps.

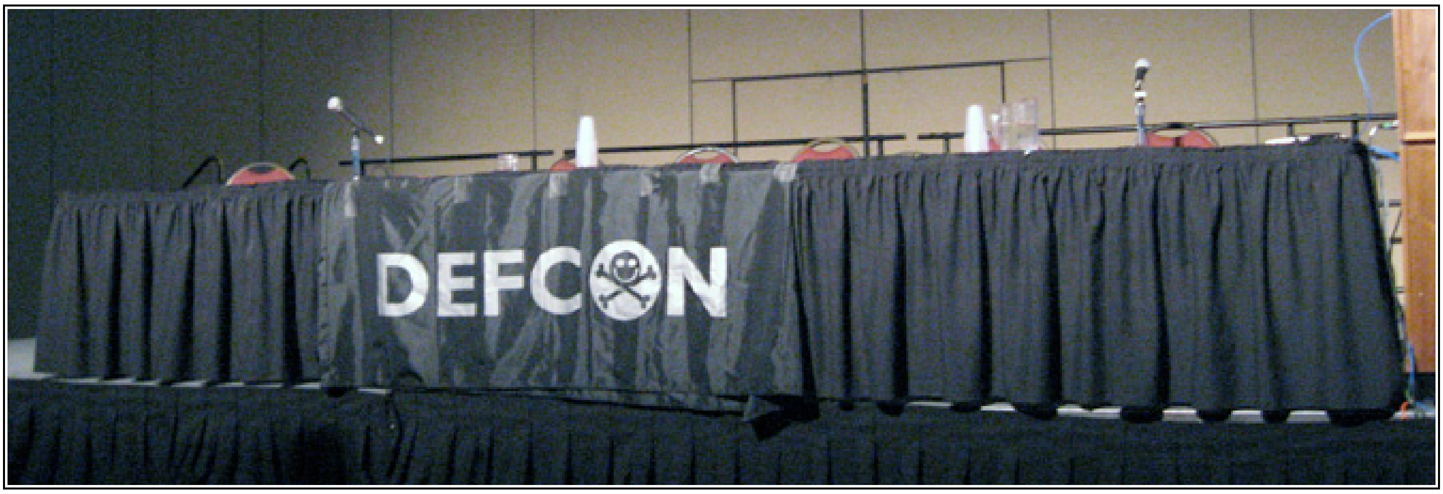
Track 1

GREG CONTI

Upload videos at http://dctv.defcon.org/ or send via bluetooth to BluetoothWallofBLame (pin:31337)

The Vendor Area you can buy T-shirts, hats, books and lock-picking tools. Also, at the surplus stand you can buy cheap hardware (used routers, switches, laptops, IP phones, ...).

Socialization and conference entertainment is a very important part of the convention and there are many official and unofficial social events for all tastes.



Vlatko Košturjak is a security specialist from Croatia, Europe. He specialized in penetration testing and ethical hacking, IT auditing, OS/Network security hardening and ISMS development according to international security standards. He also has extensive experience in Linux on almost every platform (from PDAs to mainframes). Vlatko holds stack of Linux and Security certificates. You can reach him through his website at http://kost.com.hr.

The Story of DEFCON

http://www.net-security.org/article.php?id=1044

Jeff Moss aka Dark Tangent, the founder of DEFCON and Black Hat, tells the history of the largest hacker conference and how it all got started. Find out more about the early days of the hacking scene when dial-up was considered fast, how the security space changed around the conference as years went by, and discover some bizarre things that take place at the event.

The State of Database Security

http://www.net-security.org/article.php?id=1024

Ted Julian is the VP of Marketing and Strategy at Application Security Inc. In this video he discusses the current state of database security and offers some insight on what the future holds.

Anomaly-Based Unsupervised Intrusion Detection

http://www.net-security.org/article.php?id=1013

Stefano Zanero talks about anomaly-based unsupervised intrusion detection. In this video he provides an overview of his research into the subject by illustrating how he worked trying to find ways to detect intruders without relying on signatures.

Subscribe to the HNS YouTube channel at
www.youtube.com/helpnetsecurity

File format fuzzing

By Michael Sutton, Adam Greene and Pedram Amini

File format fuzzing is a specialized fuzzing method with specifically defined targets.

These targets are usually client-side applications. Examples include media players, Web browsers, and office productivity suites. However, targets can also be servers, such as antivirus gateway scanners, spam filters, and even regular e-mail servers. The end goal of file format fuzzing is to find an exploitable flaw in the way that an application parses a certain type of file. An impressive number of client-side file format parsing vulnerabilities were uncovered in 2005 and 2006, many by nefarious parties as a number of 0day exploits were discovered in the wild prior to the typical vulnerability disclosure process. The eEye security research group does an excellent job detailing such exposures in their Zero-Day Tracker. There are a number of factors indicating that the majority of these discoveries were uncovered through file format fuzzing. This class of bugs is far from extinct, making file format fuzzing a very interesting and "hot" topic.

Here we present various methods of approaching file fuzzing, as well as talk about the different ways certain targets will accept input. Finally, we demonstrate some common vulnerabilities a file fuzzer will encounter and suggest ways of detecting such vulnerabilities in practice. The first step of course, is to choose a suitable target.

Targets

Just like traditional types of fuzzing, many different types of vulnerabilities can be found with file format fuzzing. There are also many different types of exploitation scenarios. For example, some situations will require an attacker to send a malicious file to a user and have him or her open it manually. Other situations will only require a user browsing to an attacker-controlled Web page. Finally, some situations can be triggered by simply sending a malicious e-mail through a mail server or antivirus gateway. This last scenario was the case with the Microsoft Exchange TNEF vulnerability mentioned in Table 11.1 along with other file format vulnerability examples.

Application category	Vulnerability Name	Advisory
Office productivity suites	Microsoft HLINK.DLL Hyperlink Object Library Buffer Overflow Vulnerability	tippingpoint.com/security/advisories/TSRT-06-10.html
Antivirus scanners	Kaspersky Anti-Virus Engine CHM File Parser Buffer Overflow Vulnerability	idefense.com/intelligence/vulnerabilities/display.php?id=318
Media players	Winamp m3u Parsing Stack Overflow Vulnerability	idefense.com/intelligence/vulnerabilities/display.php?id=377
Web browsers	Vulnerability in Vector Markup Language Could Allow Remote Code Execution	microsoft.com/technet/security/Bulletin/MS06-055.mspx
Archiving utilities	WinZip MIME Parsing Buffer Overflow Vulnerability	idefense.com/intelligence/vulnerabilities/display.php?id=76
E-mail servers	Microsoft Exchange TNEF Decoding Vulnerability	microsoft.com/technet/security/Bulletin/MS06-003.mspx

You will find that most targets will fit into one of these categories. Some applications fit into several categories by way of their secondary functions. For example, many antivirus scanners will also include libraries to decompress files, allowing them to act as archiving utilities. There are also some content scanners that claim to analyze image files for pornographic content. These programs can also be considered as image viewers! It is not uncommon for applications to share common libraries, in which case a single vulnerability can affect multiple applications. Consider, for example, the vulnerability detailed in Microsoft Security Bulletin MS06-055, which affects both Internet Explorer and Outlook.

Methods

File format fuzzing is different than other types of fuzzing in that it is typically performed entirely on one host. When conducting Web application or network protocol fuzzing, you will most likely have at least two systems, a target system and a system on which your fuzzer will run. The increased performance achieved by being able to fuzz on a single machine makes file format fuzzing a particularly attractive approach for vulnerability discovery.

With network-based fuzzing, it is often evident when an interesting condition has occurred in the target application. In many cases, the server will shut down or crash outright and no longer be reachable. With file format fuzzing, mainly when fuzzing client-side applications, the fuzzer will be continually restarting and killing the target application so a crash might not be recognizable to the fuzzer without proper monitoring. This is an area where file format fuzzing is more complex than network fuzzing.

With file format fuzzing, the fuzzer will generally have to monitor the target application for exceptions with each execution. This is generally accomplished by using a debugging library to dynamically monitor handled and unhandled exceptions in the target application, logging the results for later review. At the 50,000-foot view, a typical file fuzzer will follow these steps:

1. Prepare a test case, either via mutation or generation (more on this later).
2. Launch the target application and instruct it to load the test case.
3. Monitor the target application for faults, typically with a debugger.
4. In the event a fault is uncovered, log the finding. Alternatively, if after some period of time no fault is uncovered, manually kill the target application.
5. Repeat.

File format fuzzing can be implemented via both generation and mutation methods. Although both methods have been very effective in our experiences, the mutation or “brute force” method is definitely the simpler to implement. The generation method or “intelligent brute force” fuzzing, although more time consuming to implement, will uncover vulnerabilities that would otherwise not be found using the more primitive brute force approach.

Brute Force or Mutation-Based Fuzzing

With the brute force fuzzing method, you need to first collect several different samples of your target file type. The more different files you can find, the more thorough your test will be. The fuzzer then acts on these files, creating mutations of them and sending them through the target applications parser. These mutations can take any form, depending on the method you choose for your fuzzer. One method you can use is to replace data byte for byte. For example, progress through the file and replace each byte with 0xff. You could also do this for multiple bytes, such as for two- and four-byte ranges. You can also insert data into the file as opposed to just overwriting bytes. This is a useful method when testing string values. However, when inserting data into the file, be aware that you might be upsetting offsets within the file. This can severely disrupt code coverage, as some parsers will quickly detect an invalid file and exit.

Checksums can also foil brute force parsers. Due to the fact that any byte change will invalidate the checksum, it is quite likely that the parsing application will gracefully exit, providing an error message before a potentially vulnerable piece of code can ever be reached. The solution for these problems is to either switch to intelligent fuzzing, which is discussed in the next section, or as an alternative approach, disable the checks within the target software. Disabling the software checks is not a trivial task and generally requires the efforts of a reverse engineer.

Why is this method simple to use once it is implemented? That’s easy. The end user doesn’t need to have any knowledge of the file format and how it works. Provided they can find a few sample files using a popular search engine, or by searching their local system, they are essentially done with their research until the fuzzer finds something interesting.

There are a few drawbacks this fuzzing approach. First, it is a very inefficient approach and can therefore take some time to complete fuzzing on a single file. Take, for example, a basic Microsoft Word document. Even a blank document will be approximately 20KB in size. To fuzz each byte once would require creating and launching 20,480 separate files. Assuming 2 seconds per file, it would take more than 11 hours to complete and that’s only for trying a single byte value. What about the other 254 possibilities? This issue can be sidestepped somewhat through the usage of a multi-threaded fuzzer, but it does illustrate the inefficiency of pure mutation fuzzing. Another way to streamline this fuzzing approach is to solely concentrate on areas of the file that are more likely to yield desired results, such as file and field headers.

The primary drawback to brute force fuzzing is the fact that there will almost always be a large piece of functionality that will be missed, unless you have somehow managed to gather a sample file set containing each and every possible feature. Most file formats are very complex and contain a multitude of permutations. When measuring code coverage,you will find that throwing a few sample files at an application will not exercise the application as thoroughly as if the user truly understands the file format and has manually prepared some of the information about the file type. This thoroughness issue is addressed with the generation approach to file fuzzing, which we have termed intelligent brute force fuzzing.

Intelligent Brute Forge or Generation-Based Fuzzing

With intelligent brute force fuzzing, you must first put some effort into actually researching the file specifications. An intelligent fuzzer is still a fuzzing engine, and thus is still conducting a brute force attack. However, it will rely on configuration files from the user, making the process more intelligent. These files usually contain metadata describing the language of the file types. Think of these templates as lists of data structures, their positions relative to each other, and their possible values. On an implementation level, these can be represented in many different formats.

If a file format without any public documentation is chosen for testing, you, as the researcher, will have to conduct further research on the format specification before building a template. This might require reverse engineering on your part, but always start with your good friend Google to see if someone else has done the work for you. Several Web sites, such as Wotsit's Format, serve as an excellent archive of official and unofficial file format documentation. An alternate but complementary approach involves comparing samples of the file type to reveal some patterns and profile some of the data types being used. Remember that the effectiveness of an intelligent fuzz is directly related to your understanding of the file format and your ability to describe it in a generic way to the fuzzer you are using.

Once a target and method have been determined, the next step is to research appropriate input vectors for the chosen target.

THE EFFECTIVENESS OF AN INTELLIGENT FUZZ IS DIRECTLY RELATED TO YOUR UNDERSTANDING OF THE FILE FORMAT.

Inputs

With a target application selected, the next step is to enumerate the supported file types and extensions as well as the different vectors for getting those files parsed. Available format specifications should also be collected and reviewed. Even in cases where you only intend to perform a simple brute force test, it is still useful to have knowledge of the file formats you have as possible candidates. Focusing on the more complex file types can be lucrative, as implementing a proper parser will be more difficult, and therefore the chances of discovering a vulnerability arguably increase.

Let's consider an example and see how we might gather inputs. The archive utility WinRAR4 is a popular archive utility that is freely available. An easy way to tell what files WinRAR will handle is to simply browse the WinRAR Web site. On the main WinRAR page, you will find a list of supported file types. These include zip, rar, tar, gz, ace, uue, and several others.

Now that you have a list of the file types that WinRAR will handle, you must pick a target. Sometimes, the best way to pick a target is to look up information about each file type, and go with the one that is most complex. The assumption here is that complexity often leads to coding mistakes. For example, a file type that uses a number of length tagged values and user-supplied offsets might be more appealing than a simpler file type that is based on static offsets and static length fields. Of course, there are plenty of exceptions to this rule as you will find once you get some fuzzing under your belt. Ideally, the fuzzer will eventually target every possible file type; the first one chosen is not necessarily important, however it is always a nice payoff to find interesting behavior in your first set of fuzz tests for a particular application.

Vulnerabilities

When parsing malformed files ,a poorly coded application can be susceptible to a number of different classes of vulnerabilities. This section discusses some of these vulnerability classifications:

- DoS (crash or hang)
- Integer handling problems
- Simple stack/heap overflows
- Logic errors
- Format strings
- Race conditions.

Denial of Service

Although DoS issues are not very interesting in client-side applications, you need to keep in mind that we can also target server applications that must remain available for security and productivity purposes. This includes, e-mail servers and content filters. Some of the most common causes of DoS issues in file parsing code in our experience have been out of bound reads, infinite loops, and NULL pointer dereferences.

Integer Handling Problems

Integer overflows and “signedness” issues are very common in binary file parsing. Some of the most common issues we have seen resemble the following pseudo-code:

```
[...]
[1] size            = read32_from_file();
[2] allocation_size = size+1;
[3] buffer          = malloc(allocation_size);
[4] for (ix = 0; ix < size; ix++)
[5]      buffer[ix] = read8_from_file();
[...]
```

This example demonstrates a typical integer overflow that results in a memory corruption. If the file specifies the maximum unsigned 32-bit integer (0xFFFFFFFF) for the value size, then on line [2] `allocation_size` gets assigned as zero due to an integer wrap. On line [3] ,the code will result in a memory allocation call with a size of zero. The pointer `buffer` at this stage will points to an under allocated memory chunk. On lines [4] and [5], the application loops and copies a large amount of data, bounded by the original value for `size`, into the allocated buffer, resulting in a memory corruption.

This particular situation will not always be exploitable. Its exploitability is dependent on how the application uses the heap. Simply overwriting memory on the heap is not always enough to gain control of the application. Some operation must occur causing the overwritten heap data to be used. In some cases, integer overflows like these will cause a non-heap-related crash before heap memory is used. This is just one example of how integers can be used incorrectly while parsing binary data. We have seen integers misused in many different ways, including the often simpler signed to unsigned comparison error. The following code snippet demonstrates the logic behind this type of vulnerability:

```
[0] #define MAX_ITEMS 512

[...]

[1] char buff[MAX_ITEMS]
[2] int size;

[...]

[3] size = read32_from_file();
[4] if (size > MAX_ITEMS)
[5]    { printf(“Too many items\n”);return -1; }
[6] readx_from_file(size,buff);

[...]

/* readx_from_file: read ‘size’ bytes from file into buff */
[7] void readx_from_file(unsigned int size, char *buff)
{
[...]
}
```

This code will allow a stack-based overflow to occur if the value size is a negative number. This is because in the comparison at [4], both size (as defined on [1]) and MAX_ITEMS (as defined on [0]) are treated as signed numbers and, for example, -1 is less than 512. Later on, when size is used for copy boundaries in the function at [7], it is treated as unsigned. The value -1, for example, now is interpreted as 42949672954294967295. Of course, the exploitability of this is not guaranteed, but in many cases depending on how the `readx_from_file` function is implemented, this will be exploitable by targeting variables and saved registers on the stack.

Simple Stack and Heap Overflows

The issues here are well understood and have been seen many times in the past. A typical scenario goes like this: A fixed size buffer is allocated, whether it be on the stack or on the heap. Later, no bounds checking is performed when copying in oversized data from the file. In some cases, there is some attempt at bounds checking, but it is done incorrectly. When the copy occurs, memory is corrupted, often leading to arbitrary code execution.

Logic Errors

Depending on the design of the file format, exploitable logic errors might be possible. Although we have not personally discovered any logic errors during file format vulnerability research, a perfect example of this class of vulnerabilities is the Microsoft WMF vulnerability addressed in MS06-001. The vulnerability was not due to a typical overflow. In fact, it did not require any type of memory corruption, yet it allowed an attacker to directly execute user-supplied position-independent code.

Format Strings

Although format string vulnerabilities are mostly extinct, especially in open source software, they are worth mentioning. When we say mostly extinct, we say that because not all programmers can be as security aware as the folks at US-CERT, who recommend that to secure your software, you should Not Use the “%n”Format String Specifier.

But seriously, in our personal experiences, we have actually found several format string-related issues while file fuzzing. Some were discovered in Adobe 9 and Real Networks 10 products. A lot of the fun in exploiting format string issues comes from being able to use the vulnerability to leak memory to aid exploitation. Unfortunately, with client-side attacks using malformed files, you rarely are afforded this opportunity.

A FUZZER CAN UTILIZE SEVERAL SOURCES OF INFORMATION TO FIND OUT MORE INFORMATION ABOUT A PROCESS.

Race Conditions

Although people don’t typically think of file format vulnerabilities occurring due to race conditions, there have been a few that do and there are probably many more to come. The main targets for this type of vulnerability are complex multithreaded applications. We hate to target just one product in specific, but Microsoft Internet Explorer is the first application that comes to mind here. Vulnerabilities caused by Internet Explorer using uninitialized memory and using memory that is in use by another thread will probably continue to be discovered.

Detection

When fuzzing file formats you will typically be spawning many instances of the target application. Some will hang indefinitely and have to be killed, some will crash, and some will exit cleanly on their own. The challenge lies in determining when a handled or unhandled exception has occurred and when that exception is exploitable. A fuzzer can utilize several sources of information to find out more information about a process:

- *Event logs*. Event logs are used by Microsoft Windows operating systems and can be accessed using the Event Viewer application. They are not terribly useful for our purposes,as it is difficult to correlate an event log entry with a specific process when we are launching hundreds during a fuzz session.
- *Debuggers*. The best way to identify unhandled and handled exceptions is to attach a debugger to the target application prior to fuzzing. Error handling will prevent obvious signs of many errors caused by fuzzing but these can generally be detected using a debugger.
- *Return codes*. Capturing and testing the return code of the application, although not always as accurate or informative as using a debugger, can be a very quick and dirty way to determine why an application ended. Under UNIX at least, it is possible to determine which signal caused an application to terminate via the return code.

- *Debugging API*. Instead of leveraging a third-party debugger, it is often feasible and effective to implement some rudimentary debugging features into the fuzzer itself. For example, all we will be interested in knowing about a process is the reason it terminated, what the current instruction was, the register state, and possibly the values in a few memory regions like at the stack pointer or with respect to some register. This is often trivial to implement, and is invaluable in terms of time saving when analyzing crashes for exploitability.

Once a given test case has been determined to cause a fault, make sure to save the information that was gathered by whatever fault monitoring method you choose in addition to the actual file that triggered the crash. Saving test case metadata in your records is important as well. For example, if the fuzzer was fuzzing the 8th variable field in the file and it was using the 42nd fuzz value, the file might be named file-8-42. In some cases, we might want to drop a core file and save that as well. This can be done if the fuzzer is catching signals using a debugging API. Specific implementation details regarding this can be found in the next two chapters.

Summary

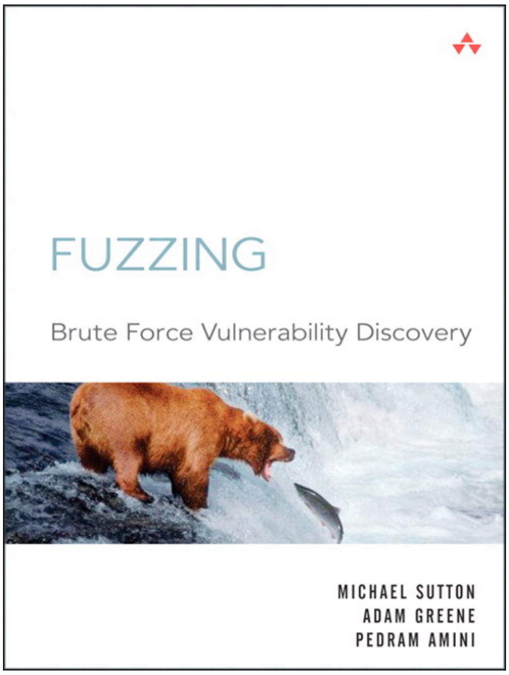
Although file format fuzzing is a narrowly defined fuzzing method, there are plenty of targets and numerous attack vectors. We have discussed not only the more traditional client-side file format vulnerabilities, but even some “true remote” scenarios, such as antivirus gateways and mail servers. As more and more emphasis is placed on preventing and detecting network-based attacks over TCP/IP, file format exploits still remain as a valuable weapon to penetrate internal network segments.

Michael Sutton is the Security Evangelist for SPI Dynamics. He is a frequent speaker at major information security conferences, has authored numerous articles and is regularly quoted in the media on various information security topics.

Adam Greene is an engineer for a large financial news company based in New York City. His interests in computer security lie mainly in reliable exploitation methods, fuzzing, and UNIX based system auditing and exploit development.

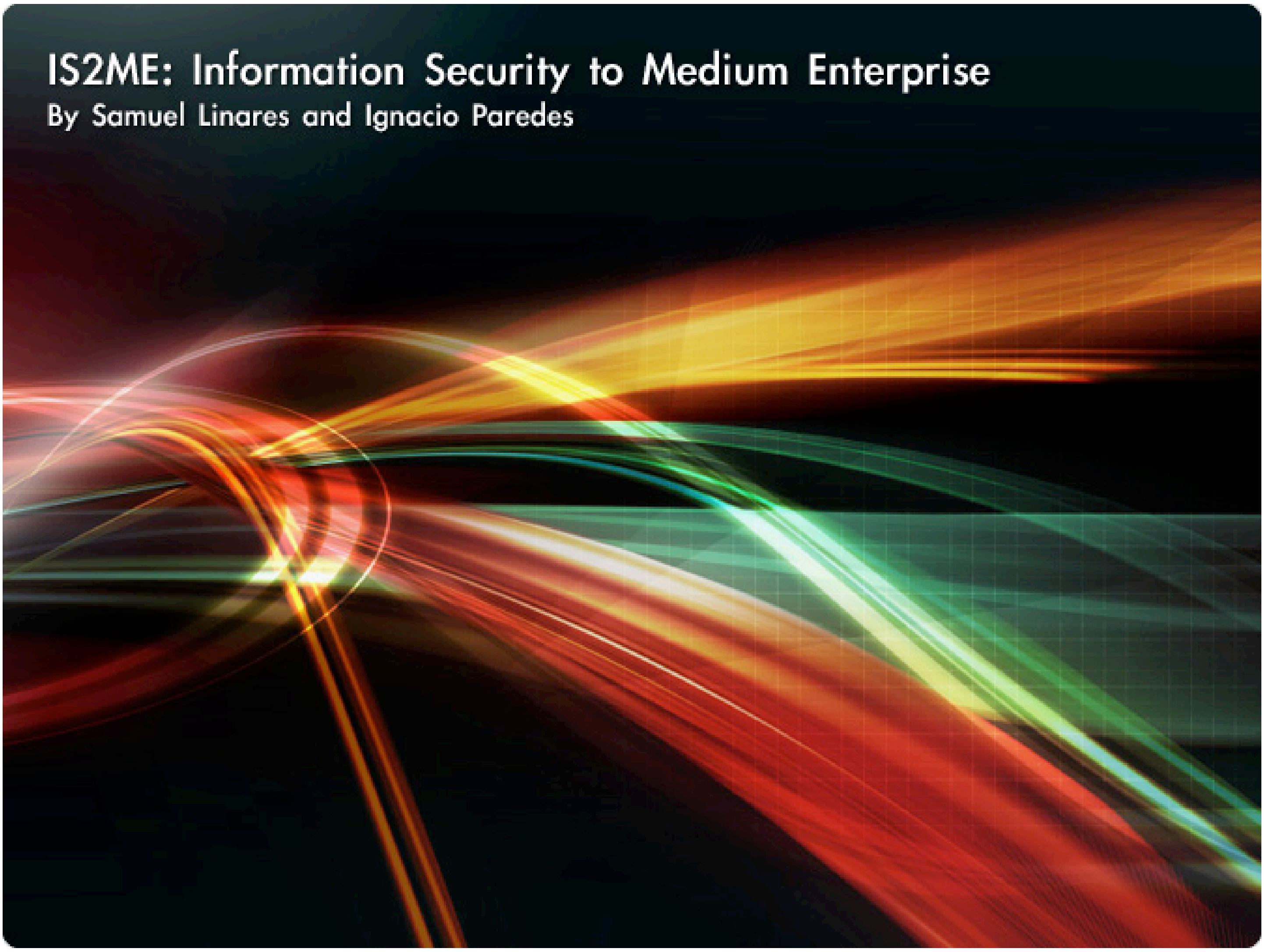
Pedram Amini currently leads the security research and product security assessment team at TippingPoint. He spends much of his time in the shoes of a reverse engineer- developing automation tools, plug-ins and scripts.

This article is an excerpt from the Addison-Wesley book “Fuzzing: Brute Force Vulnerability Discovery” and you can find out more about it in the “Latest addition to our bookshelf” section in this issue of (IN)SECURE.



IS2ME: Information Security to Medium Enterprise

By Samuel Linares and Ignacio Paredes



Small and medium enterprises include more than 90% of worldwide enterprises and more than 99% of the enterprises in the European Union. Existing methodologies and standards about security management require an infrastructure and a resources investment that in the majority of the cases does not exists and it is not within reach to this kind of organizations.

Usually, in such organizations, an adequate organizational structure is missing and in most of the cases it lacks a Chief Security Officer, whose job is assumed by the IT manager (systems and/or communications). This fact, joined to the lack of knowledge about information security, leads to a very basic, and insufficient, deployment of security measures, most of them made punctually to solve an existing problem or necessity in the organization.

Daily labour does not allow the people involved to have a global view or make an adequate planning and management of information security. This in turn leads to a lack of commitment from the top-level management regarding these issues. This inevitably makes the organization assume an unacceptable level of risk, which will unfortunately carry out security incidents or non-compliance issues and therefore have an undesirable impact on business. This is the moment where the need for information security professionals arises in the organization. They are needed in order to solve existent problems and start the long way towards the decrease of risk and the deployment of adequate security measures.

When the incidents occur, companies used to mark essential requirements such as immediate results about risk decreasing and short term critical security measures deployment. Without doubt, the development of an action plan project is also requested.

This action is intended to allow the top-level management and the security manager (in fact the IT manager) to identify which resources are needed, and what is the proper way to include security as an additional requirement in the business processes of the organization.

This is a complex challenge that the information security professional could approach in a traditional fashion following the typical methodologies and standards (mainly ISO 27001), and consequently starting a classical ISMS implementation process.

The strict execution of these phases in small and medium enterprises uses to be quite complicated due to the lack of commitment from top-level management and the absence of a minimal information security structure. The deployment of security measures (controls) does not start until the project is quite advanced (probably months after the start), and because of this, one of the objectives of the company, the short term critical measures deployment, is not achieved.

This scope is accurate and right, despite it is accepted as the medium or long-term path to follow, and is not commonly accepted by companies, which are looking forward short-term immediate results ("we want security and we want it now").
Here arises the need for a methodology or approach to scenarios like those outlined before. This approach should provide a bridge between total non-compliance and a methodological deployment of security management according to a standard like ISO 27001.

This is the reason of presenting IS2ME (Information Security to the Medium Enterprise) as an approach and solution to outline the path to follow towards the deployment of information security in organizations whose security model is not mature enough. IS2ME will allow these organizations the desire to undertake security deployment and its associate management system in an efficient, effective, practiced way, which allows short-term risk decreasing, and start the accomplishment of the required standards.

IS2ME also pursuits an ambitious social objective: the approaching of information security to medium (and small) enterprises, encouraging its penetration and reducing the general level of risk, and hence increasing its value, revenues and economic level of the majority of organizations that exist nowadays.

The IS2ME method has as its main objective the rapid decreasing of the Information Security risk taken by the organization.

1. Objectives

The IS2ME method has as its main objective the rapid decreasing of the Information Security risk taken by the organization. By the adoption of technical and organizational measures within a framework, several steps need to be developed in order to execute a defined project. The last aim of the project is the achievement of security bound to the usual operations of the organization, just as an additional requirement of the business processes. This is going to simultaneously allow the obtaining of short-term results that lead to identify the actual state of the organization's security, the needed tasks to increase it and the action plan for its implementation.

2. The Method

From a broad view, IS2ME starts evaluating the security of the organization by collecting information through interviews with personnel, field tests and technical analysis. This information is compiled in a report that states the level of implantation of the different security measures. As a result of the report, a proposal for an action plan is produced. After its approval by top-management, its development and implementation will be carried out, establishing a basis and starting the long way towards compliance and implantation of the Information Security Management System according to ISO 27001.

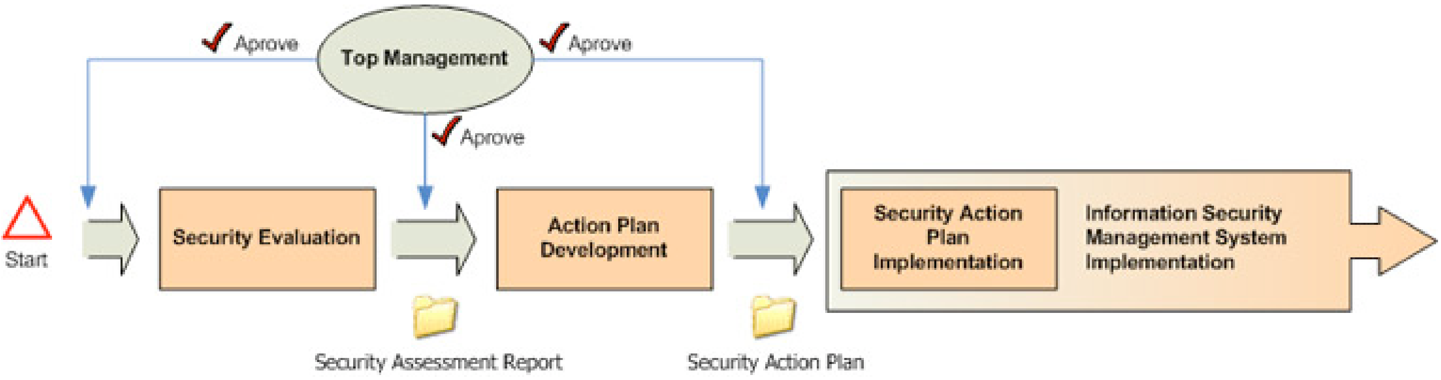

Aprove
Top Management
Aprove
Aprove
Start
Security Evaluation
Action Plan Development
Security Action Plan Implementation
Information Security Management System Implementation
Security Assessment Report
Security Action Plan

Figure 1

During the development of IS2ME, we have tried to follow a holistic and extremely practical oriented approach that allows the user a simple and immediate enforcement just by following a set of sequential well-defined phases showed in the next graphic and described in detail in the following sections.

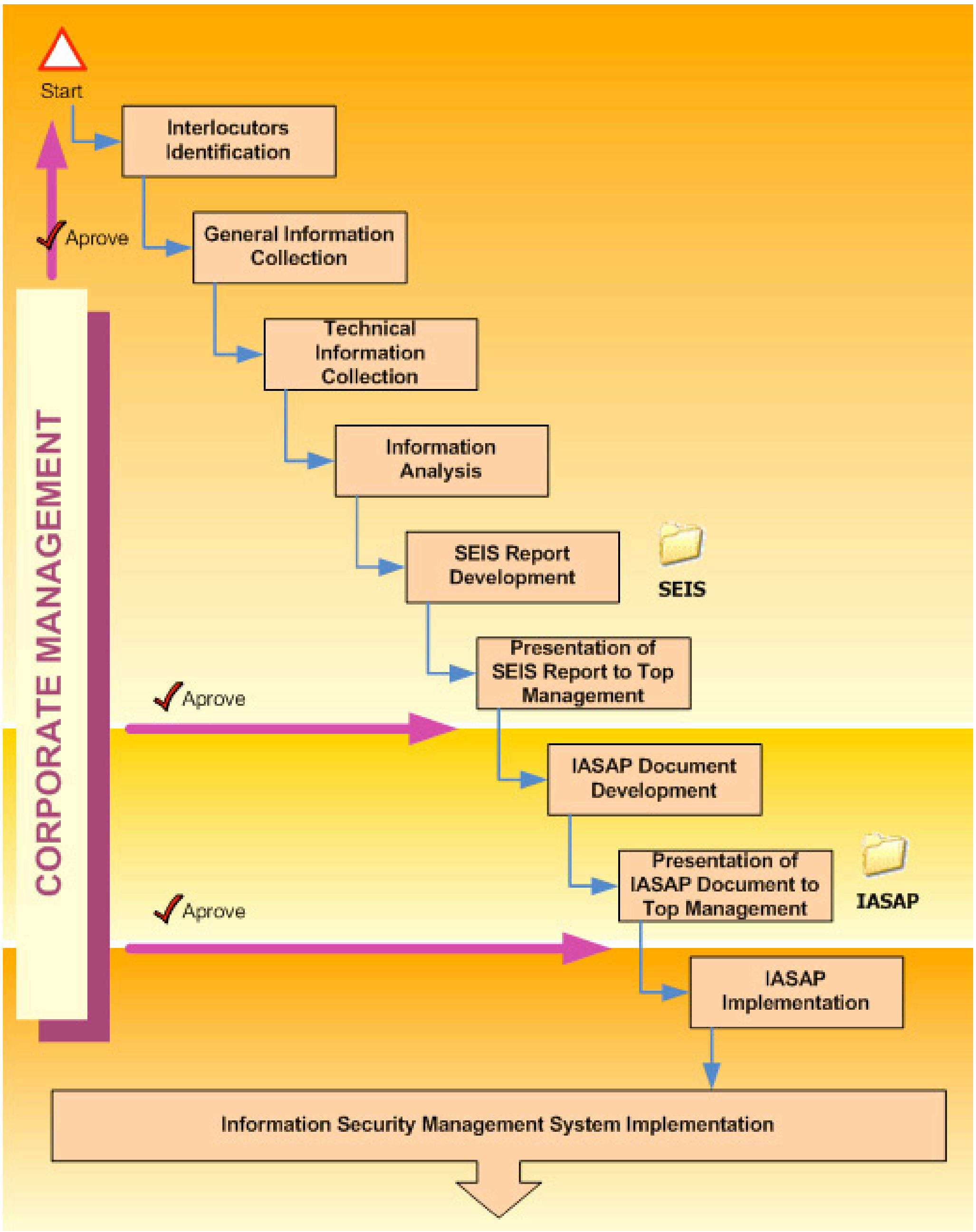

Start
Interlocutors Identification
Aprove
General Information Collection
Technical Information Collection
Information Analysis
SEIS Report Development
SEIS
Presentation of SEIS Report to Top Management
Aprove
CORPORATE MANAGEMENT
IASAP Document Development
Presentation of IASAP Document to Top Management
IASAP
Aprove
IASAP Implementation
Information Security Management System Implementation

Figure 2

2.1 Interlocutors Identification

Objective: To identify valid interlocutors in the organization and to plan their availability during subsequent tasks.

The information collection phase has great importance in the development of the method since this information is going to be the source of the analysis and subsequent tasks, and will lead to the development of the action plan. For that reason, during the whole development of this phase, it is very important to have deep involvement by the organization to obtain the information needed.

The work team must sign a confidentiality and non-disclosure agreement, in order to provide the organization a warranty about the proper use of the collected data. On the other side, the organization should provide a signed authorization for the work team to make any checks and tests needed to carry out the planned tasks.

2.2 General Information Collection

Objective: To obtain all kinds of information through interviews, documentation reviews and similar methods related to information security, that should include technical, organizational and compliance information.

The initial phase collects information as a source for tests and analysis. During this phase a significant interaction occurs between the organization and the work team. Staff of the work team will be present in facilities of the organization to allow a fluid dialogue and ease the obtaining of the needed information. Therefore, an appropriate workspace should be provided as well as interlocutor availability.

Before the work team is to be present in the facilities of the organization, a questionnaire could be provided to the interlocutor who, with the help of key people in the organization, should return it to the work team properly answered. In this way, the work team could focus its efforts during the period of presence in the organization facilities in order to maximize to results and minimize the amount of time used during the information collection phase.

During this phase, information is obtained about technical aspects such as network topologies, services, existing security devices, addressing plans, and organizational and compliance aspects such as authority matrixes, organizational charts, policies and procedures, and description of current compliance regarding information technologies.

2.3 Technical Collection of Information

Objective: To obtain all kinds of information through different technical and empirical methods in order to get representative samples from systems and devices across the organization.

Next, pointed out are the different points that should be executed during the technical collection of information.

2.3.1 Enumeration and Characterization

Starting from the general information collected during the General Collection of Information phase, the systems, devices and applications object of the technical study are identified developing an exhaustive characterization of every identified element that should include name of the system/application, vendor, location, person in charge, software versions patches, associated systems, etc.

2.3.2 Traffic Analysis

The aim of traffic analysis is to characterize the kind of traffic that is usually carried by the networks in the organization, as well as detect possible failure points or bottlenecks in these networks.

2.3.3 Systems and Applications Vulnerability Assessment

The applications and systems vulnerability assessment has as objective to detect weak security points. Weak points are programming or configuration errors in applications and the operating system that could cause vulnerabilities potentially exploited by possible attackers. Therefore, it is important to know that weak points with the purpose of deploying appropriate controls to eliminate them or avoid its exploitation.

2.3.3.1 Remote Analysis

Special attention needs to be paid to vulnerabilities that could be exploited remotely, since this implies a bigger risk since they do not require physical presence for its exploitation. These vulnerabilities usually are linked to application ports waiting for remote connections. The first step in the vulnerability assessment, therefore, is to identify which are the ports in the systems that can be accessed remotely.

The analysis will not only include devices that are accessible from the Internet, but also accessible devices from different logical security zones within the organization.

2.3.3.2 Local Analysis

The purpose of the local analysis is to provide accurate knowledge about the state of security in the system. This kind of analysis is not usually available to potential attackers, but can give very useful information to know the state of the system from the point of view of security. In brief, we try to obtain the most accurate characterization of the system.

2.3.4 Configuration Review

During the technical collection of information, the configuration files of key elements in the network are reviewed. Many times, due to the high number of devices in the network it is not be possible to make an exhaustive review, so it is necessary to select, according to the interlocutor in the organization what are the key devices whose configuration is going to be reviewed.

For the process of reviewing the configurations, you will probably need the help of experts in order to be able to identify configuration failures, configurations that are more efficient or alternatives to allow the improvement of security and efficiency of the device.

Typically, reviewed will be network devices (routers, switches, bridges, etc.), security devices (firewalls, IDS/IPS, authentication servers), applications (web, FTP, mail servers, etc.) and any device which could be a source of vulnerabilities and therefore increase the risk level in the organization.

2.3.5 External Visibility

A large amount of information related to organizations is available to the public. This information could be a key piece in the design of an attack plan because it can reveal interesting details, both technical and organizational. Therefore, it is important to the organization to be conscious about the existence of this information. Special attention should be paid to issues such as public addressing, the domain name system and documentation filtering.

Special attention needs to be paid to vulnerabilities that could be exploited remotely.

2.4 Information Analysis

Objective: To study and analyze the information that has been collected in previous phases, according to best practices, standards, methodologies, knowledge and experience of the work team.

After collecting general and technical information, a complete analysis of all the collected information should be made.

The analysis studies possible lacks of information security in products, network designs, accesses to information, processes and others according to codes of good practices, methodologies and standards. Of course, the expertise and knowledge of the work team in charge of the project it is also a key issue.

This analysis is a step before the development of the State of Enterprise Information Security Report (SEIS Report) that will develop all the findings and recommendations of the product analysis.

2.5 SEIS Report Development (State of Enterprise Information Security)

Objective: To produce a report about the state of information security within the organization. This report is in a simple and concise way a snapshot about the current state of the organization about the deployment of technical and organizational measures regarding information security.

This report looks forward two objectives. The first one is to provide a global and detailed point of view about the state of the organization regarding information security. The second objective is to point out the improvable aspects about information security, and propose corrective actions, prioritized according with its importance inside the organization. Next, the different sections in the SEIS report are described:

2.5.1 Current State Description

In this section, the findings discovered during the Technical Collection of Information are described, as well as the current state of communication networks and information systems within the organization. An example structure for this section could be: topology, systems, services, physical security, logical security, operations and management.

2.5.2 Analysis and Technical Recommendations

For each one of the subsections remarked in the previous section, and following the same structure, the existing implications regarding information security needs to be reviewed, and recommendations proposed in order to solve the problems that have been found.

2.5.3 Conclusions and Action Proposals

In this section, recommended actions marked in the last section are ordered following a gradation based on the critical level of their application.

Special attention should be paid to actions marked as extremely urgent, because they suppose a high and immediate level of risk that cannot be taken by the organization. For every recommended action, a time frame for its execution is proposed.

2.5.4 Security Measures and Recommended Controls

Additionally, a series of applicable measures and security controls are proposed such as existing good practices guides.

2.5.5 Executive Summary

The executive summary should be developed as a section of the report. It should list in a clear and simple way, and using a language lacking technical terms, a summary of the main results.

2.6 Presentation of the SEIS Report to Top Management

Objective: To present the report about the State of Enterprise Information Security to top-level management. This is a milestone for the organization taking security as one more of its actual objectives.

The SEIS report will serve as a reference to top management to support its decisions made about decreasing the risk taken by the organization. This report should be presented to top management in order to identify key messages avoiding, where possible, technical terms.

2.7 Development of IASAP Document (Information Assurance and Security Action Plan Document)

Objective: To produce the Information Assurance and Security Action Plan Document that will serve as foundation for the deployment of recommended actions and development of the security plans.

The approval of the SEIS report from top management should include explicitly the acceptation of the development of the IASAP document (Information Assurance and Security Action Plan). Once received, the development of the IASAP document should start, approaching in detail each one of the actions proposed in the SEIS report.

Proper security measures and actions must be selected and deployed in order to decrease risk to an acceptable level. These actions and security measures are the ones previously identified in the SEIS report, and are going to be developed in detail in the IASAP document, including required resources for its deploying, planning and economic valuation.

The IASAP document will be the basis to the organization's Information Security Action Plan. The document should include a complete planning of the deployment of identified actions so that dates and milestones could be established for the fulfillment and attainment of organizational, departmental, and even personal objectives across the organization. For each of the actions, there's information such as technical development, complete planning, needed resources identification, economic valuation and suppliers offerings when external support is needed.

The actions to include in the IASAP document are dependent on the security measures already deployed by the organization and the degree of penetration of information security inside the organizational culture. These actions include aspects such as improvement of organizational structure, improvements in systems and data centers, development of business continuity process, and more. In some cases, should it be necessary, even advisable, the support from third parties.

2.8 Presentation of the IASAP Document to Top Management

Objective: To present the Information Assurance and Security Action Plan to Top Management for its approval, in order to establish a foundation for its late deployment.

Once finished, the presentation of the IASAP document should be made to top management. This presentation should have been planned in advance during the presentation of the SEIS report, and set continuity on the execution of the project to deploy security, which is the main objective of this method.

Approval of the IASAP document by top management is a key milestone in the commitment of the organization about the integration of information security in all its processes, since this approval means the start of the Information Security Action Plan according to corresponding features, planning and estimation of human and economic resources.

Outlined below, as an example and reference, is a proposed schema of the presentation of the IASAP document:

- Introduction about the origins of the IASAP document and its development process.

- Justified description of short, medium and long terms, and the inclusion of tasks in these time frames.

- Short Term: Detailed description of each task to be made in this term, including time frame of deployment, needed resources (marking if they are internal of external), providers proposals where needed, included tasks and economic valuation. (For example, tasks that should be executed in a term shorter than six months).

- Medium Term: Detailed description of each task to be executed as stated in the previous point. (6 to 12 months).

- Long Term: Detailed description of each task to be executed as stated in the previous point. (more than 12 months).

- Time planning proposal: Proposal with real dates about the fulfillment of objectives stated in the IASAP document.

2.9 IASAP Implementation

Objective: To develop and deploy the Information Assurance and Security Action Plan according to the proposed planning.

Once the IASAP document is presented and accepted by management, it is time to start the execution of the different tasks outlined in the Information Assurance and Security Action Plan. Although the involved personnel in the development of the different phases of the IS2ME method do not have to be totally dedicated to the execution of these tasks, it is important for them to make monitoring and coordination tasks in order to assure that objectives are achieved and the controls are correctly deployed.

This is a very important step, because the correct resolution of the proposed tasks will allow the organization to start the long path towards compliance and implantation of an ISO 27001 Information Security Management System. At this moment, a traditional approach on information security management could be approached.

In order to execute the IASAP, a Coordination Project Plan needs to be developed which include acquisition and allocation of needed resources and monitoring of the tasks specified in the action plan as well as periodical review meetings.

Conclusions

Lately, the corporate World has started to be conscious about the necessity to incorporate security into the organizations. This is a non-trivial hard task. Fortunately, there are methodologies that ease the development of the process to allow it. Nevertheless, most of the times, these methodologies suppose that the organizations have a dimension, resources and previous work done which is not the case in most of the organizations.

The authors think that IS2ME could fill an empty space in the implantation of security in small and medium enterprises, allowing, on the contrary of traditional methodologies, the rapid obtaining of results with a reasonable employment of resources. These results will mean a decrease in the risk faced by the organization, the elimination of a big amount of organizational and technical problems, and a solid foundation to allow the implantation of the security measures in order to lead to a full implantation of an Information Security Management System.

More information and free download of IS2ME can be obtained from the official web site: www.is2me.org

Samuel Linares is a senior security consultant and security manager with Tecnocom, with +10 years of security, system integration and project management experience. He leads and has created all the security services offered by Tecnocom, the 3rd bigger IT company in Spain, implementing a lot of security solutions in customers, including compliance audits, penetration tests, ethical hacking, firewalls and IPSs deployments or security network designs. He holds various certifications including GIAC Assessing Wireless Networks (GAWN), Systems and Network Auditor (GSNA), and Google Hacking & Defense (SSP-GHD), BSI BS 7799 Lead Auditor, Juniper JNCIA-FW, Checkpoint CCSE & CCSA, Sun SCNA & SCSA, among others. Samuel holds a B.S. in Computer Science from the Univ. de Oviedo and is University Specialist in Data Protection by the Colegio Universitario Escorial Maria Cristina.

Ignacio Paredes works as senior security consultant with Tecnocom, he has wide experience in leading and developing information technology related projects. For the last years he has been deeply involved in different aspects of information security such as secure network design and deployment, access control technologies and methodologies, or information security management systems development. He holds several security related certifications such as GIAC Assessing Wireless Networks (GAWN), Systems and Network Auditor (GSNA), and Google Hacking & Defense (SSP-GHD), EC-Council Certified Ethical Hacker (CEH), BSI BS 7799 Lead Auditor, Sun SCNA & SCSA. Ignacio holds a Master’s Degree in Computer Science from the Universidad de Oviedo.

The authors can be reached by e-mail:

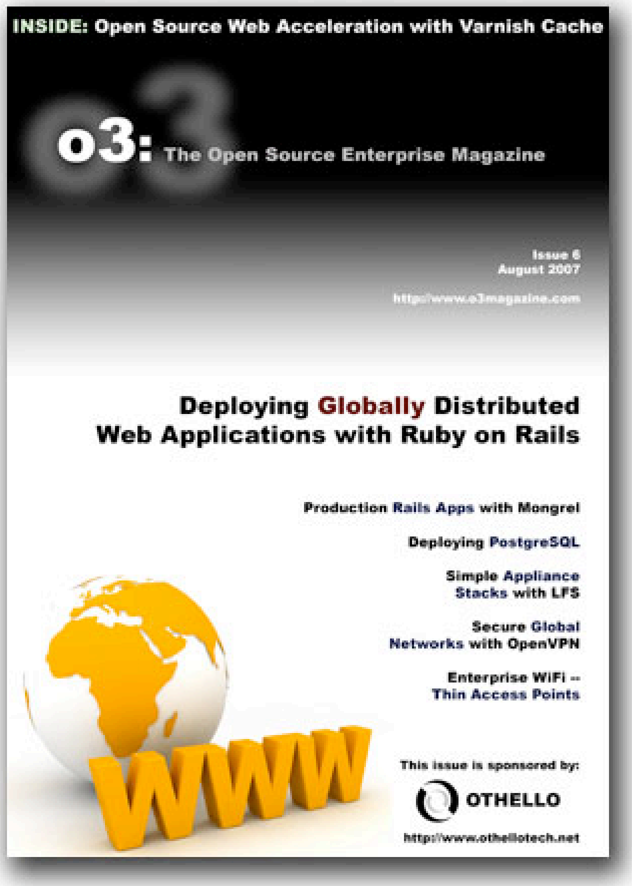
Samuel.linares@tecnocom.es

Ignacio.paredes@tecnocom.es

o3: magazine

Open Source / Enterprise
Free DIGITAL magazine

http://www.o3magazine.com



INSIDE: Open Source Web Acceleration with Varnish Cache

o3: The Open Source Enterprise Magazine

Issue 6
August 2007

http://www.o3magazine.com

Deploying Globally Distributed Web Applications with Ruby on Rails

Production Rails Apps with Mongrel

Deploying PostgreSQL

Simple Appliance Stacks with LFS

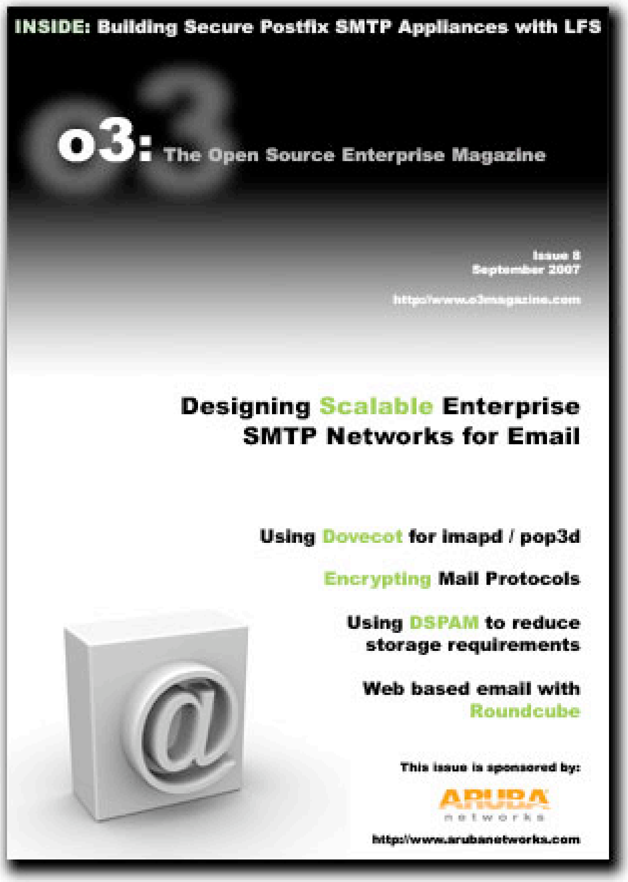
Secure Global Networks with OpenVPN

Enterprise WiFi -- Thin Access Points

This issue is sponsored by:

OTHELLO

http://www.othellotech.net



INSIDE: Building Secure Postfix SMTP Appliances with LFS

o3: The Open Source Enterprise Magazine

Issue 8
September 2007

http://www.o3magazine.com

Designing Scalable Enterprise SMTP Networks for Email

Using Dovecot for imapd / pop3d

Encrypting Mail Protocols

Using DSPAM to reduce storage requirements

Web based email with Roundcube

This issue is sponsored by:

ARUBA networks

http://www.arubanetworks.com