

the security journal

“Common Sense Security for Common Businesses”



IN THIS ISSUE:

The Global Security Syndicate
Information Security Practice

Incident Response, Part 6

A CVE-Based Security Mgmt Model

Windows XP Embedded Security



5350 Tomah Drive
Suite 3500
Colorado Springs, CO
80918

<http://www.securityhorizon.com>

Editor in Chief: Russ Rogers

The Security Journal is always on the lookout for quality writers for this publication. If you're interested in submitting an article for inclusion in an upcoming edition of The Security Journal, please contact Russ Rogers at russr@securityhorizon.com.

Cover photo courtesy of Joe Grand,
Grand Idea Studio, Inc.



<http://www.grandideastudio.com>

Special Layout Editor: Michele Fincher

For more information on Security Horizon, please visit our web site or email us at: info@securityhorizon.com.

Security Horizon, Inc. was founded in 2000 and is headquartered in Colorado Springs, Colorado. As a company, we believe that sound security services are based on education, experience, standards, ethics and unquestionable integrity.

Table of Contents:

Notes from the Editor

By Russ Rogers.....p.3

Incident Response Part 6: Follow-Up

By Greg Miles.....p.5

NSA IAM Course Schedule

.....p.7

A CVE-Based Security Management Model

By Robert A. Martinp.9

NSA IEM Course Schedule

.....p.13

Information Security Practice

By Shelley Keating.....p.15

The Global Security Syndicate

By Greg Miles.....p.17

Windows XP Embedded Security

By Travis L. Schack.....p.20

Special thanks go out to Ping Look from **Look Designs** for the creation of the new Security Horizon logo and the new cover masthead images for The Security Journal.

For more information on Look Designs:
www.republicofping.com
design@republicofping.com

All content used by permission or
Copyright 2000-2004,
Security Horizon, Inc.

Rediscover Security.

Illuminate your mind. Gain knowledge. Learn the threats of tomorrow, today.
Be challenged by the experts who are doing innovative work. Meet and network with
thousands of your peers from all corners of the world at the Black Hat Briefings USA 2004—
the only technical security event to offer you the best of all worlds.



Black Hat®

Briefings & Training USA 2004

July 24-29, 2004 • Caesars Palace Las Vegas

Training: 4 days, 19 topics • Briefings: 2 days, 9 tracks, 60 speakers

www.blackhat.com

for updates and to register or call +1.916.853.8555

sponsors

diamond



platinum



gold



silver



Notes From the Editor



Russ Rogers
CISSP, CISM
Editor in Chief

Greetings! I write this edition of Notes from a cramped and uncomfortable airline seat somewhere in row 11 on a flight from Atlanta to Denver. We're returning from the popular Techno-Security conference in Myrtle Beach, SC. And as I sit here, sore from the apparently wooden seat beneath the 70's era décor seat covering, I wonder why this seemingly new airline has not seen beyond the façade of modern greed long enough to realize that there is yet room for evolution.

That's what really got me to thinking. The security industry, as new and innovative as we may seem, lacks the ability to evolve. If you take a look back a few years, things were pretty much the same as they are right now. We had the firewalls and intrusion detection. We had anti-virus software and configuration monitors. But back then, it was still fairly new and we all felt secure in the idea that the industry, as a whole, was moving forward and making the world a better place.

But consider the changes that have really occurred over the past few years. We have more companies in the information security space than ever before. Each one believing that they have the latest and greatest cure for the woes of cyberspace. But folks, we're still talking firewalls, intrusion detection, and anti-virus. Heck, even the security services organizations have failed to truly evolve.

Now before someone out there throws a gasket, yes, there are some really great

companies out there. But we still need innovation. We still need standardization by consensus. With the sheer number of snake oil salesmen in the security realm trying to hock their wares to unsuspecting and naïve consumers, we're all going to pay the piper if the industry leaders don't stand up and start taking action.

There are really two basic areas that I take issue with. The first area is the product industry. We're rehashing old products. Sure, there are minor advances as each company releases a new "technology", but the monetary value of intellectual property, combined with the potential for revenue generation, ensures that the executives of these corporations hoard their ideas away instead of sharing the simple concepts with the community at large.

The second area relates specifically to an area that Security Horizon competes within; professional services. Professional services are apparently a very easy place to start a new company. I've seen more new companies in this area over the past few years than I thought possible. But when we take a step back and look at these organizations, how many are performing security for their customers haphazardly, versus a standard and repeatable approach? And how are you, as the customer supposed to pick the charlatans from the professionals?

So as I sit here sipping my obligatory orange juice, munching my tasteless pretzels, and staring down at the corn fields below anxiously; I'm also considering my options. What can I do to actually make a difference? Well, let me tell you what we've got in mind.

It's called the Global Security Syndicate, or GSS for short. It's not a company. No one in this organization is out to make a lot of money off of this venture. GSS exists for the good of

Notes From the Editor, cont.

humanity. Now how's that for innovation?
<wink>

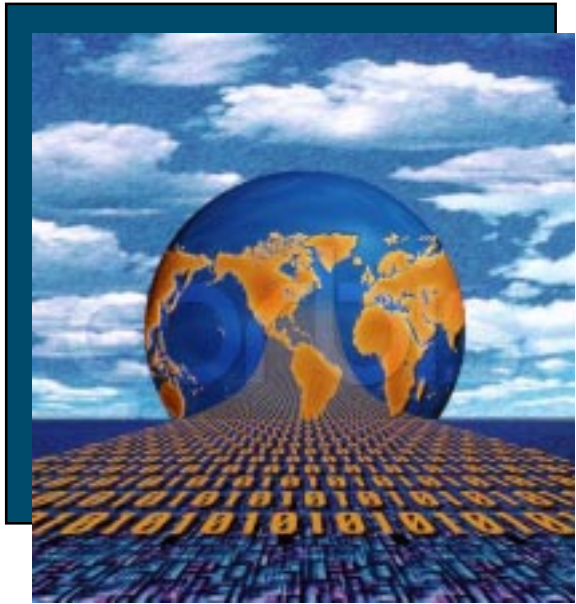
GSS is an organization supported by member organizations. The money earned within GSS stays within GSS for research, development, and creation or endorsement of public standards. The companies involved will all be highly regarded for their contributions to the world of information security. One of the first projects being undertaken by the GSS is a public standard for the education of security professionals while they're still in school. As security certifications become more diluted with each and every passing day, customers have no means to adequately measure the knowledge base of security professionals. The same is true for the large security companies that employ security professionals. Just because someone has a CISSP or has received a SANS certification doesn't mean they will be able to provide a quality end product.



So, for the security professionals or product developers out there reading this, consider this article your call to arms. This is a challenge to you. Change the world. Make it a better and safer place. And if you're interested in hearing more about the GSS and what it's about, check out the article from Greg Miles in this issue of the Journal. For the customers out there reading this, take a deep breath. The ethical, moral, and innovative side of information security is making a come back.

So with the flight attendant standing over me, waiting patiently for my empty wrapper and half consumed orange juice can, I say goodbye.

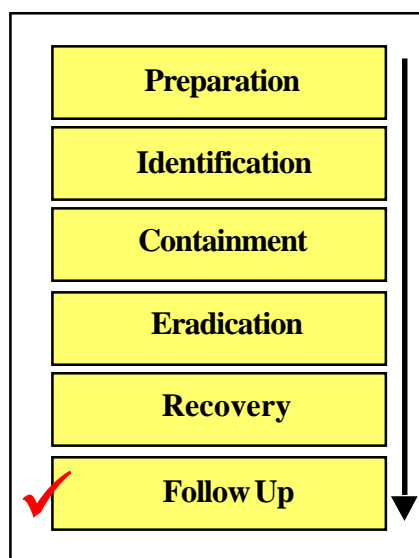
Peace and best wishes to you all.



“Just because someone has a CISSP or has received a SANS certification doesn't mean they will be able to provide a quality end product.”

Last issue we took a look at the recovery process and the critical steps to restore the systems and/or servers to full operation after a security incident. This article is the final of a six part series in Incident Response (IR). IR professionals have adopted a basic core set of activities that encompass the IR discipline that includes IR preparation, identification, containment, eradication, recovery, and follow-up.

Professional organizations that provide advice in the IR arena include but are not limited to the Carnegie Mellon Software Engineering Institute CERT® Coordination Center (www.cert.org), the SANS Institute (www.sans.org), National Information Protection Center (www.nipic.gov), Federal Computer Incident Response Center (www.fedcirc.gov), and the Forum for Incident Response Security Teams (FIRST) (www.first.org). This article focuses on IR Follow-Up.



The Incident Response Process

Through the previous five (5) Incident Response Articles, our focus was preparing for and implementing the incident response process to get back to operation. The follow-up phase is to be conducted after the completion of either an incident response test or the completion of an actual incident response. While you typically do not have to touch the affected system(s) during this final phase, it is still a crucial step in maintaining an effective Incident Response program.

During the Follow-Up Phase, you will focus on the following:

- Assure all reporting and final documentation are complete from the incident
- Turn over any additional required information to the organizations legal counsel or law enforcement
- Determine incident costs
- Meet with the Incident Response Team to review the IR process for flaws and lessons learned
- Determine any adjustments or improvements to existing policy, processes and/or procedures

Final Documentation Completed: No process or project is complete until the final documentation is closed out. This includes

any trouble tickets that were started, the primary incident response reports, and any updates to management. This final documentation may also include public relations contacts to get the word out to investors and customers that the problem has been fixed. This is especially important in HI visibility situations that may have a negative image impact on the organization. If personal information about individuals, clients, or investors was compromised or potentially compromised by the security incident, the organization may be legally and/or ethically required to notify the individuals of this possible compromise. If the organization is not legally required to notify others, then it becomes an organizational decision on who is notified. It may be wise to consult with your legal counsel when deciding on the notification process to assure liability concerns are addressed. Final documentation of the incident provides a means to track all activities from the incident, the amount of effort put into addressing the incident, what actions were taken, and how the incident was closed out. Many incident reports will show the final level of effort put into the incident to track trends and costs. This information will be extremely important from both a budgeting and a prosecution process.

Working with Legal Counsel/Law Enforcement: If a formal investigation resulted from the security incident, the

organization may be required to support legal requests and law enforcement for a considerable amount of time following the incident. The organization should be prepared to provide logs, reports and details on the incident, as well as assuring the integrity of this information by protecting the evidence related to the incident. This evidence may be used in prosecution.

Incident Costs: It is important for the organization to track the cost of the incident both in personnel and equipment costs to get an accurate representation of what the average incident costs over time. This information is also important to assist law enforcement in making their case and can drive whether an incident will be prosecuted or not, and under what laws the incident can be prosecuted.

Review Lessons Learned: The IR process should be implemented as a continuous process improvement model that will help organizations to implement better procedures while handling incidents. This process normally includes a meeting with the IR team to discuss what went right and what went wrong during the handling of the incident. Did the right people get contacted? Was it timely? Was the infrastructure protected properly during the handling of the incident? Did other entities get called in correctly? (i.e. law enforcement, support vendors, etc.) The



Incident Response Part 6

lessons learned process provides the means to validate the current processes and identify areas that need improvement. The organization should document these lesson learned in detail so they can be applied to the process either in policy, procedures, and/or training.

Make Changes and Improvements:

Based on the lessons learned, implement changes to the IR process that will make it more efficient, effective, and manageable. Realistically, you can expect the first 2 or 3 incidents will result in major changes the overall IR processes and procedures. This is another reason why testing your IR process is so critically important to a successful IR program

By the time you finish with the follow-up process, you may already be in the middle of your next incident. Don't let this final step be forgotten. Assure it is done with as much vigor and effort as the other five phases or you will ultimately end up making the same costly mistakes over and over again.

As I have stated in every single article on Incident Response to date, **Preparation** (see article: Incident Response Part 1: Preparation) is still the most important step in the incident response process.

© Security Horizon Inc. 2004

Gregory S. Miles, Ph.D., CISSP, CISM, is the President of Security Horizon Inc. and a regular contributor to the Security Journal.

Contact him at greg@securityhorizon.com.



7/24-7/25, 2004	Las Vegas, NV Black Hat USA
7/26-7/27, 2004	Las Vegas, NV BlackHat USA
8/6-8/7, 2004	Omaha, NE NEbraska CERT
8/23-8/24, 2004	Sierra Vista, AZ
8/26-8/27, 2004	Kansas City, MO
9/14-9/15, 2004	Colorado Springs
9/27-9/28, 2004	Orlando, FL

The IAM is a two-day course for experienced Information Systems Security analysts who conduct, or are interested in conducting INFOSEC assessments of U.S. Government information systems. The course teaches NSA's INFOSEC assessment process, a high-level, non-intrusive process for identifying and correcting security weaknesses in information systems and networks.

FREE 1 Year license to the SAINT Vulnerability Scanner just for attending any of our courses!

IAM training so good that even our competitors attend **our** classes!

To register for one of these courses or to get further information, please contact us at:

(719) 488-4500
info@securityhorizon.com
<http://www.securityhorizon.com>



How Vulnerable are Your Networks?

Find out with

SAINT®

NETWORK VULNERABILITY SCANNER

Two new ways to scan ...

SAINTbox™
APPLIANCE SCANNER



Just plug into your network and your vulnerability worries are over. For more information visit:
www.saintcorporation.com

WebSAINT®
ON-LINE SCANNER



A quick easy way to get SAINT's reliable results with no downloading or configuring. Scan from
www.saintcorporation.com

SAINT® is certified CVE-compatible by MITRE and winner of PC Magazine's 4-Star award.

A CVE-Based Security Management Model By: Robert A. Martin

Security management including risk assessment, exposure identification and vulnerability management is a process that involves a large number of elements, which, traditionally, were not easily exchanged and integrated. The CVE effort, lead by the MITRE Corporation has introduced a naming process that helps keep vulnerabilities under control.

Introduction

Security vulnerabilities are now much more common than, say, six years ago, however, that is not to say that they were not present. Vendors such as Sun, and Cisco produced security alerts and the CERT was created in 1988, after the Morris worm took down part of the Internet. At that time, and until recently, each and every one of the players in the security vulnerabilities arena, from independent security investigators that disclosed vulnerabilities to vendors that patched those in their systems, used their own naming scheme when referring to their vulnerabilities.

When a new vulnerability was disclosed, vendors would issue advisories telling administrators to update their systems, security software would be updated in order to detect attempts to exploit that issue (in the case of intrusion detection systems) or to detect if the issue is present (in the case of patch management software or vulnerability assessment scanners). However, how could a security manager know if a given vulnerability had been fixed in the systems under his responsibility? How could he forward the information on the vulnerability in such a way that other (non-security) personnel could determine if the vulnerability was patched or needed to be patched? At that time, there was really no way to correlate the information from all those different sources, if a vulnerability scanner was run, the resulting

report might not be useful to system administrators since they might not be able to determine which precise patch was needed to fix the vulnerability. If an attack was detected it was difficult to determine if that attack was directed towards a system that had already been patched for the attack (and thus, the alarm needed to be downgraded) or if it was still exposed and, consequently, the alarm needed to be immediately treated since the attack might have been successful.

This situation resulted in a "tower of Babel" making it difficult for the personnel managing security within organisations. As an example, take a look at Table 1, which shows how a single vulnerability (the issue with the phf CGI program) was named by different providers (vulnerability databases, and vendors of security software).

Vulnerability Management with CVE

The Common Vulnerabilities and Exposures (CVE) is an international, community-based effort, including industry, government, and academia, has created an organizing mechanism to make identifying, finding, and fixing software product vulnerabilities more rapid and efficient. The MITRE Corporation, who started the effort, is a not-for-profit company that works in the public interest to provide systems engineering, research and development, and information technology support to the U. S. government. In January 1999, a paper [1] presented in the 2nd

A CVE-Based Security Management Model By: Robert A. Martin

Table 1 - Vulnerability Tower of Babel, 1999

Organization	Name referring to vulnerability
AXENT (now Symantec)	phf CGI allows remote command execution
BindView	#107—cgi-phf
Bugtraq	PHF Attacks—fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CA-96.06.cgi_example_code
Cisco Systems	HTTP—cgi-phf
CyberSafe	Network: HTTP 'phf' attack
DARPA	0x00000025 = HTTP PHF attack
IBM ERS	ERS-SVA-E01-1996:002.1
ISS	http—cgi-phf
Symantec	#180 HTTP server CGI example code compromises http server
SecurityFocus	#629—phf Remote Command Execution Vulnerability

Workshop on Research with Security Vulnerability Databases at Purdue University outlined the concept of the Common Vulnerabilities and Exposures Initiative (<http://cve.mitre.org>). The result of this initiative is the CVE list, a mechanism to link the different tools, concepts and software involved in a security process as shown in Figure 1.

The CVE list is made up of CVE names, which are unique names for every publicly known information security vulnerability and exposure. The CVE list is commonly thought of a vulnerability database, but it's not. It's a

dictionary, unique vulnerabilities are included in that dictionary in such a way that one can ask: what is the name for this vulnerability? And get a single answer and like a dictionary, synonyms for the vulnerabilities are also listed.

The CVE effort had first to answer the question: what is really a vulnerability? The term "vulnerability" is a rather broad term. For example, if a system is running a service that provides information that it should not provide (a service that lists all the users of an organisation), is this really a vulnerability?



Figure 1 - Cross-Linking through the CVE List

A CVE-Based Security Management Model By: Robert A. Martin

What if the service is doing what it is supposed to do (give a list of users) but it really should not be installed (per the organisation's policy). CVE decided to draw the line between a vulnerability, which are only called vulnerabilities if they are indeed "universal": they don't depend on your security policy and are considered a problem in reasonable security policies, and exposures, which are those vulnerabilities that are violations of a given security policy and might, or might not, be considered a vulnerability in different security policies.

Once this terminology [3] was agreed on the CVE effort started developing the CVE list. This is a time-consuming process since MITRE and the CVE Editorial Board, the group responsible for the content of the list, needs to determine if a vulnerability disclosed by a researcher or a vendor has been previously published (i.e. it matches a vulnerability already in the list) and, if it has not, is a single vulnerability or it is made of more than one vulnerability which needs to be assigned different names. The new entries in the CVE list start as candidates (still under review) and are published in order to not delay the vulnerability publication process; these candidates are then reviewed by the board members and will end up becoming an official CVE entry. The time candidates take to become entries varies and depends on how clear or obscure the vulnerability might be.

Vendors and organisations are encouraged to ask for, and include, CVE names in their advisories and public announcements when new vulnerabilities are disclosed. This introduces CVE in the vulnerability management process right from the start.

CVE in the Security Management Process
CVE improves the security management

process in many ways, by assigning a unique identifier it is possible to track the cycle of vulnerabilities within an organisation and, as a consequence, manage the risk associated with them:

- detect vulnerabilities that affect the organisation's systems, through the software that is installed within them (with patch management software) or through the advisories published by vendors
- reduce the risk related to vulnerabilities in those systems, either by fixing them (patch installation) or reducing the risk associated from someone that exploits that vulnerability by introducing safeguards
- monitor the use of those vulnerabilities to try to leverage access to a system (impact) and determine what is the probability of impact given the status of the vulnerability and the safeguards introduced to mitigate it.

A CVE-enabled process is shown in Figure 2 and exemplifies the use of CVE in order to mitigate risk. In the process, an attack targeted towards the organisation's system is detected by the IDS, the vulnerability assessment tool might have previously determined whether the systems are vulnerable to the attack or not. Regardless on whether the system is "thought" to be vulnerable, the patch management system, which can use the information provided by the vendor, has the final knowledge of that fact. This information can be combined together and, as a result, the organisation can know whether the attack has:

- a) targeted a vulnerability that does not exist on the system (it is not present, it is already fixed, it has been reduced by some other safeguard...)
- b) targeted a vulnerability that does exist on the system

A CVE-Based Security Management Model By: Robert A. Martin

The answer of the organisation is dependant on whether the attempt succeeded or not and without a common naming process for vulnerabilities throughout the full system there is no way all that data can be properly correlated. That's the main benefit of CVE for security management.

order to search for CVE names

Additionally, there are additional requirements for tools, services and databases of security information. The CVE compatibility process is made up of two phases, a first one in which the organisation declares its use of CVE

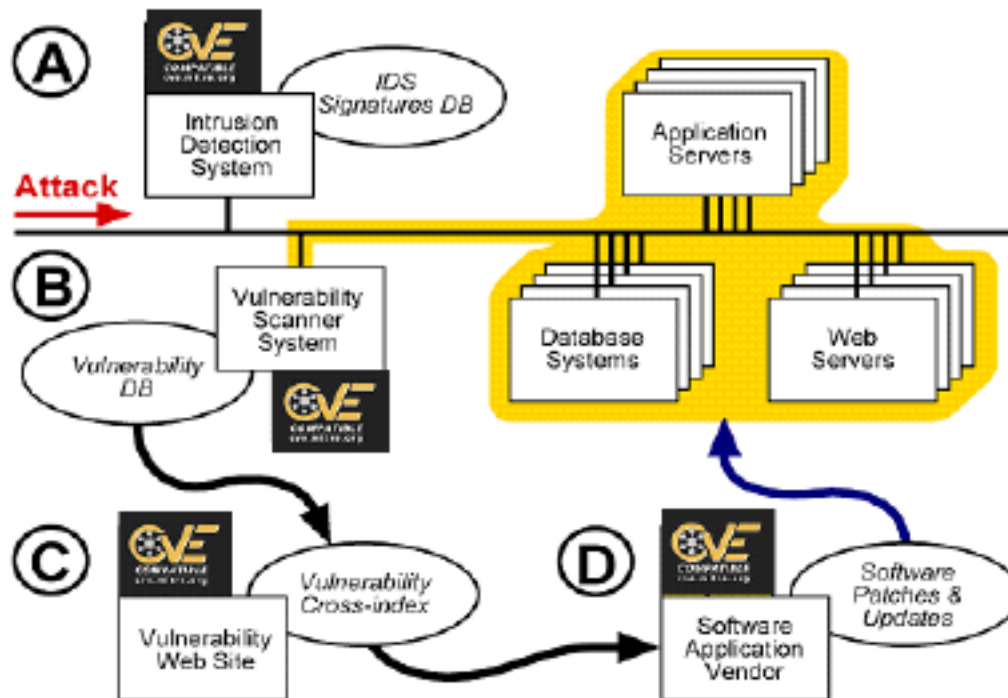


Figure 2 - A CVE-Enabled Process

CVE Compatibility

Of course, in order to be able to do this process, tools, and information sources, need to provide information in a standard way. That's the main reason why the CVE effort includes a CVE-compatibility effort to acknowledge and assess information sources and vendors use of the CVE standard.

Being "CVE-compatible" in a service, information source or product means:

- using CVE names properly
- being accurate with respect to CVE names usage
- providing users with reports including CVE information
- providing users with an interface in

names (this phase started in October 1999) and a second one (started in May 2003) in which MITRE evaluates whether the organisation complies with the CVE standards. Currently 192 different products of 119 organisations in 18 different countries have started this process of CVE compatibility.

Conclusions

CVE is currently approaching the goal of uniquely naming every publicly known security relevant software mistake. More than half of all known software mistakes are now either included on the CVE List or are under review. And journals refer to CVE names when comparing scanners and IDS as a desirable

A CVE-Based Security Management Model By: Robert A. Martin

feature. The U. S. National Institute for Science and Technology (NIST) has published a recommendation to all federal government agencies and services for the use of CVE-compatible products and services whenever possible and the U. S. Department of Defense issued Directive 8500.2, Information Assurance (IA) Implementation Instruction, includes "For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention". It is surprisingly uncommon to find an effort in the security arena that is supported by information security tool vendors, software developers and companies offering information security related services. CVE is an international community-based effort that has improved how organisations can efficiently manage risk and work with the information of many different sources and vendors. If you are a security manager, you should consider taking advantage in CVE in order to improve your own risk and vulnerability management process. If you are a tool user, demand CVE-compatibility of your vendors since it will greatly aid you in your security process.

References

[1] D. E. Mann and S.M. Christey, "Towards a Common Enumeration of Vulnerabilities," 2nd Workshop Research with Security Vulnerability Databases, Purdue University, West Lafayette, Ind., 1999; <http://cve.mitre.org/docs/ceries.html> (current June 2004).

[2] R. A. Martin, "Managing Vulnerabilities in Networked Systems," IEEE Computer Society's Computer Magazine, Vol. 34, No. 11, November 2001; <http://www.computer.org/computer/co2001/ry032abs.htm> (current June 2004).

[3] CVE Terminology: <http://cve.mitre.org/about/terminology.html> (current June 2004).

Robert A. Martin is CVE Compatibility Lead at the MITRE Corporation.

ramartin@mitre.org



The NSA IEM is here!!

The INFOSEC Evaluation Methodology (IEM) is a hands-on methodology for conducting evaluations of customer networks utilizing common technical evaluation tools. Students can expect to learn an easily repeatable methodology that provides each customer a roadmap for addressing their security concerns and increasing their security posture.

7/26-7/27, 2004	Las Vegas, NV Black Hat USA
8/9-8/10, 2004	Colorado Springs
8/12-8/13, 2004	Colorado Springs
9/13-9/14, 2004	Colorado Springs
9/16-9/17, 2004	Colorado Springs
9/29-9/30, 2004	Orlando, FL

To register for one of these courses or to get further information, please contact us at:

(719) 488-4500
info@securityhorizon.com
<http://www.securityhorizon.com>





Are you playing in the real world without the proper credentials?

A real Bachelor's or Master's degree, focused on advancing technology. Available on campus or online.
Learn more. www.uat.edu or 800.658.5744

What is security? Security is the method of protecting a system. The questions I am asked as a security professional and an educator, deal with hardware and software centric security solutions usually concerning a network. Which hardware firewall or software antivirus solution should be implemented based on a set of complex circumstances in a particular situation? There are specific answers to these types of security questions. Are the answers to these questions security? Does this mean if I find the correct solution to my hardware firewall or antivirus software that my system is secure?

The interesting component in all the security conversations is the complete lack of questions which are foundational and important. What are those important security questions? First, we need to answer the question "What is not Security?"

"What is not Security?"

- Security is not a simple answer or solution
- Security is not hardware
- Security is not software
- Security is not personnel
- Security is not product

Then, "What is Security?"

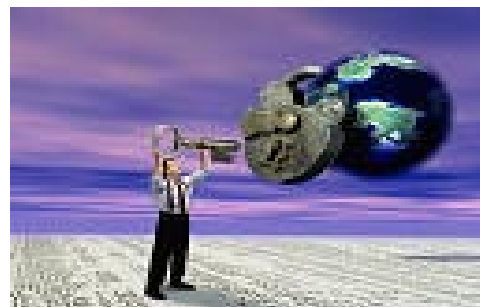
- Security is a complex web of interconnected physical, personnel, operational, communication, network, and informational systems. Each of these systems has components of software, hardware, data, people and procedures
- Security is a mindset
- Security is a cyclical process
- Security is an ongoing set of practices

ISP is like medical practice because there

are no definitive answers. There is no single authoritative manual or recipe to follow that answers every question. It would be great to purchase a single book for all your information security needs; however, such a book does not exist. Instead we must rely on experience, education, information, and trial-and-error tweaking based on our best judgment. ISP depends on the circumstances surrounding the interconnected systems and components. There are guidelines, policies, procedures and best practices. Each of these is a useful tools in securing your network; however, creating a secure environment only begins with these tools.

Lets compare the methods of a doctor's medical practice to the methods of an IS Practitioner.

When you go to your family doctor you are interviewed regarding your symptoms and the circumstances surrounding your medical complaint. The doctor formulates a diagnosis using experience and expertise. This diagnosis is the doctor's best judgment (an educated guess) as to what is wrong. Are doctors always right? No. Doctors practice the art of medicine as a scientific discipline. Doctors are continually learning and developing medical skill and expertise. Doctors are vigilant with their education because if they are not then there are disastrous consequences and the doctor has a dilemma.



What do doctors have to do with security? IS Practitioners, like doctors, must practice the art of their profession. The ability to skillfully apply education, experience, and knowledge gained from textbooks, journals, and references to keep informed about making accurate diagnosis. An IS Practitioner must rely on these same set of skills to be successful.

When you go to your IT department you are initially interviewed by the IS Practitioner (formerly known as a Systems Engineer) regarding the symptoms and the circumstances surrounding your network or security complaint. The IS Practitioner formulates a diagnosis using experience and expertise. This diagnosis is the IS Practitioner's best judgment (an educated guess) as to what is happening to the system. Are IS Practitioner's always right? No. IS Practitioners practice the art of information security as scientific discipline. How do IS Practitioners practice security? They same way doctors practice medicine. IS Practitioners must continually learn and develop skills and expertise to counter security threats. IS Practitioners must be vigilant with their education because if they are not then security breaches occur. Then it becomes time to polish your resume because you will be looking for a new job.

ISP is about the frequent and regular monitoring, updating, testing, modification, and repairing of an organization's security system. The attentive ISP includes software, hardware, data, personnel and procedures. A comprehensive security system can encompass physical, personnel, operational, communication, network, and informational systems. a technical issue and your people need to be trained and made aware of how they can help.

What are the important security questions?

- What is your procedure for frequent and regular monitoring, updating, testing, modification, and the internal and external repairing of your organization's security system?
- Does the procedure include software, hardware, data, personnel and procedures?
- Does the procedure include physical, personnel, operational, communication, network, and informational systems?
- Do you have a scheduled maintenance time? Do you follow the schedule?
- Do you monitor or assess logs? On a regular schedule?
- Do you update or modify your hardware and software systems? On a regular schedule?
- Do you perform infiltration testing of hardware and software systems? On a regular schedule?

ISP is complex. ISP is not simply adding a new piece of hardware or software on your network and proclaiming that you now have a secure environment. ISP depends on the circumstances surrounding the interconnected systems and components. This is why it is imperative that as a IS Practitioner you consider each of these questions on an individual basis. A secure environment requires a dedicated and knowledgeable Information Security Practitioner who understands the intricacies of securing and preserving the integrity of an information system.

Shelley Keating is an Information Security Practitioner and a faculty member with the University of Advancing Technology in Tempe, AZ.

<http://www.uat.edu>



Alas, a security organization not focused on profit motives. The Global Security Syndicate (GSS) (www.gssyndicate.com) is a security organization composed of members from multiple representative companies focused on improving overall international security through open source efforts on multiple projects. The GSS will host multiple security projects to gain and provide community support in standardizing some of the activities around many TBD subjects. One of the first focused projects is the open source Education Curriculum project to help both educational institutions and employers to address the kinds of knowledge students of security are expected to gain while pursuing their certificates and degrees.

GSS Mission: The Global Security Syndicate (GSS) is a global not for profit organization of security professionals and companies (products and services) dedicated to advancing Information Security practices for all levels of business and government agencies by:

- Knowledge sharing through collaborative effort of local community and industry research projects
- Increasing global security awareness and education
- Developing secure strategies and standards to enhance the security life cycle of security programs and products



GSS Board of Directors: The **GSS Board of Directors** will be composed of thirteen (13) individual global security professionals initially selected through invitation for a one (1) year term. After the initial one (1) year term, new directors will be nominated and voted on by the 13 member Board of Directors, with a majority vote required to extend an invitation to become a board member.

GSS Member Organizations: Separate from the Board of Directors is **GSS Member Organizations** that can petition to have their organization listed on the GSS website in a specific security category. The approval process for membership is under development, but is expected to include a peer review through the board of directors, as well as, reference checks specifically related to the security category the organization is applying. GSS Member Organizations will also be required to uphold a strict code of ethics.

There are multiple subcategories for most of the listed categories. The initial set of categories includes:

- **Application Security**
- **Database Security**
- **Identification/Authentication**
- **Managed Security Services**
- **Security Research and Development**
- **Assessment Services**
- **Communications Security**
- **Web Security**
- **Security Documentation**
- **Network Security**
- **Disaster Recovery**
- **Legal**
- **Education and Training**

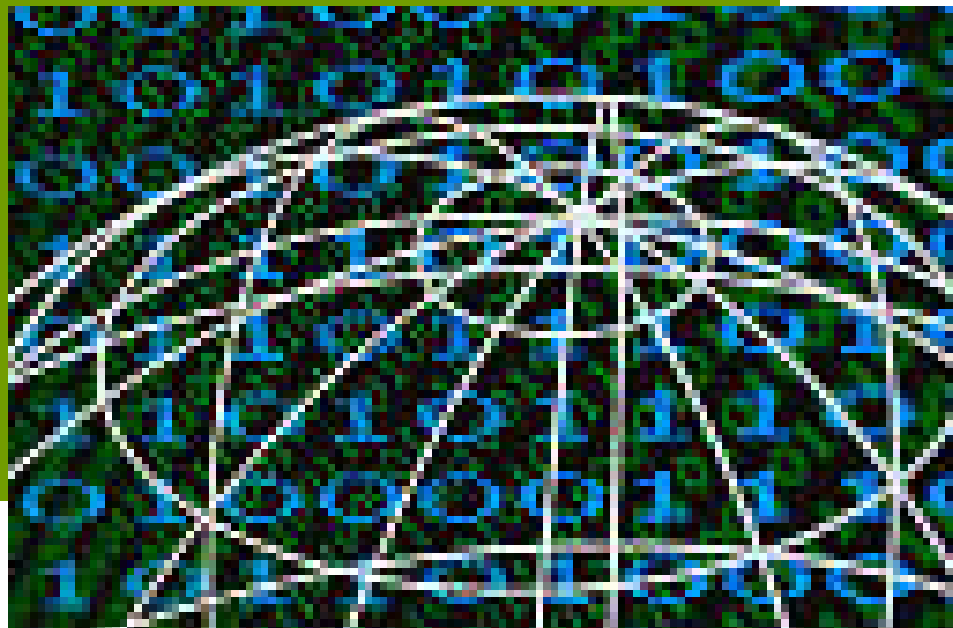
Security R&D: The other major focus of the GSS is community involvement in research and development projects that will ultimately lead to the availability of open source information on compelling security topics. Research topics may be submitted for consideration by GSS Board of Directors, GSS Member Organizations, other professional security organizations and consumers of security services.

Stay tuned as the GSS evolves. Better yet, get involved!

© Security Horizon Inc. 2004

Gregory S. Miles, Ph.D., CISSP, CISM, is the President of Security Horizon Inc. and a regular contributor to the Security Journal.

Contact him at greg@securityhorizon.com.



AVAILABLE FROM SYNGRESS PUBLISHING AND SECURITY HORIZON!

\$49.95 US
\$69.95 CAN

512 pp, 7 x 9.1875
ISBN: 1-931836-05-1



Stealing the Network: How to Own a Continent

A fictional continent is emerging as a major new economic, political and military force on the world stage. However, their rapid growth has left little in the way of time and money to sure up their Internet backbone, and it is vulnerable to a potentially catastrophic attack. Who are the bad guys? What do they want? How will it end? The only way to know for sure is to read this fascinating cyber-thriller, written by a team of the most accomplished cyber-security specialists in the world.



\$49.95 US
\$69.95 CAN

512 pp, 7 x 9.1875
ISBN: 1-931836-03-5

Wardriving: Drive, Detect, Defend

“A comprehensive and authoritative guide to WarDriving and wireless security.” –Mike Kershaw (Dragorn), Kismet author

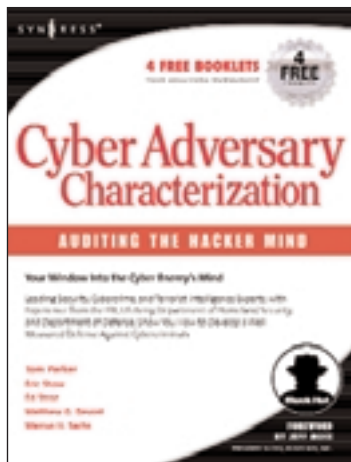
“...covers every aspect of wireless security from some of the most respected people in the wireless community. It should be on every IT person’s bookshelf.” –John Kleinschmidt, Michiganwireless.org Founder

“This is the ‘Kama Sutra’ of WarDriving literature. If you can’t WarDrive after reading this, nature has selected you not to.” –Bob “bobzilla” Hagemann, WiGLE.net CoFounder

ALSO AVAILABLE FROM SYNGRESS PUBLISHING:

\$49.95 US
\$69.95 CAN

512 pp, 7 x 9.1875
ISBN: 1-931836-11-6



Cyber Adversary Characterization

From a “hactivist” concerned with worldly politics and agendas, to a script kiddie looking for a little fun, criminal hackers are as varied, as they are skilled. CyberAdversary Inside the Mind of the answers: Who is the hacker, what do they want to hack, and why do they want to hack it?



\$49.95 US
\$69.95 CAN

512 pp, 7 x 9.1875
ISBN: 1-931836-09-4

Zero-Day Exploit

A group of highly sophisticated cyber-terrorists have developed a Zero-Day Exploit targeting critical, petrochemical infrastructure systems in the United States. Once launched, the exploit will cripple the country’s ability to respond or defend itself. The only defense against disaster rests with an elite cyber-security expert with the skill and savvy to thwart the plot.

Syngress: The Definition of a Serious Security Library™

Windows XP Embedded Security, Pt 1 By: Travis L. Schack

If you look around you, I bet you can find several devices that contain an embedded system. Embedded devices come in all sizes, from cellular phones, to PDA's, to IP set-top box, to cash registers, to ATM systems...I can go on and on! The embedded industry has exploded in the last couple of years. Yet, no vendor has been crowned as the dominant operating system in this maturing market.

This article is not about why you should use Windows XP over a proprietary OS or Linux. There are many factors that have to be considered in deciding which OS to use for your embedded device. You can find many articles on the Internet that compare Windows XP embedded with embedded Linux and some of the proprietary embedded OS's in the embedded industry. This article will provide an overview of important security issues concerning Windows XP embedded and the critical security functionality (or security deficiencies) it offers for embedded devices.



Overview

Microsoft released Windows XP embedded (XPe) in January 2002. Based on the Windows XP Pro code, you can create a customized operating system run-time image

by choosing only the functionality you require through a set of 10,000 components. If you include all components into your image, you essentially have a full working Windows XP Pro operating system.

Companies are expanding the use of XPe in areas such as consumer electronics, network gateways, instrumentation and industrial automation devices, IP set-top boxes, Kiosk/ATMs, medical devices and systems, mobile and handheld devices, portable media devices, cash registers, slot machines, security appliances, and VoIP devices.

It is beyond the scope of this article to go into detail on building a full XPe image. There are many articles and how-to documents on Microsoft's site that explain designing, building, deploying, and managing an XPe run-time image. I will provide a brief breakdown of the build process. Building a XP embedded image involves using a special installation process that essentially builds a custom-version of Windows XP for your device. You can load as many or as few features as needed by selectable operating system features (such as Windows Media® Player or Internet Explorer), services (such as networking), drivers (such as peripheral drivers), operating system features (such as Windows Media® Player or Internet Explorer), services (such as networking), and drivers (such as peripheral drivers). You can also choose the extent of networking features that would allow the device to connect to corporate networks or the Internet. Windows XPe devices connecting to other computers or the Internet are potentially susceptible to viruses, worms and other threats that face computers running the full version of the XP operating system. Increasing the security of your embedded device from these threats will result in less time and money spent cleaning up after virus infections, network Denial of

Windows XP Embedded Security, Pt 1 By: Travis L. Schack

Service attacks, system compromise and data disclosure.

As the proliferation of embedded systems continues, systems designers and programmers are aware that what they now produce must be architecturally sound, yet adaptable to future integration and add-on applications. For an embedded system to carry out its defined functions and do it securely, it is necessary to construct a consistent and structured approach for designing and building a secure embedded system.

most critical and difficult phase of the life cycle of a system. A developer or development team must carefully balance the business functional needs and objectives of the system with critical security requirements. Notice the word “carefully”. If the embedded system is too secure and cannot perform its functions, the system will be unusable. If the system is not protected properly, eventually it will not function and be unusable! Get my drift? It is critical that security be used to “enable and not disable” your embedded device.

“It is critical that security be used to ‘enable and not disable’ your embedded device.”

System Life-Cycle

The software development process must incorporate all life-cycle phases of your embedded system. The National Institute of Standards and Technology (NIST) has identified and defined 5 phases for a system life-cycle in publication “SP800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems.” NIST SP 800-27 Rev A “Engineering Principles for Information Technology Security (A Baseline for Achieving Security)”, which incorporates the 5 phases from SP 800-14, presents a list of secure engineering principles to be considered in the design, development, and operation of an information system. The Initiation and Disposal phases will not be covered in this document. We will focus on Development/Acquisition, Implementation, and Operation/Maintenance phases.

Development/Acquisition

The Development/Acquisition phase is where the system is designed and developed or purchased. This may sound simple but is the

With the explosion of the Internet, time to market of a system/product has become more valuable to a business and has drastically decreased the amount of time a development team spends on the Development and Implementation phases. Microsoft XP embedded (XPe) is marketed as “enabling you to rapidly develop reliable and full-featured connected devices”. Security is one of the highlighted features of the “full-featured” statement. In theory, only adding the components that you need for your XPe embedded image could make it secure. If you add in some or all of the components that inherent known security vulnerabilities and weaknesses of Windows XP, you will have a smaller OS footprint that is just as vulnerable as any XP system on the Internet. Rapid deployment of any system results in a large number of software defects and design oversights. It is next to impossible to add security to an existing system by adding security on top. Security must be considered and implemented from the beginning.

Windows XP Embedded Security, Pt 1 By: Travis L. Schack

To determine security requirements of your XPe system, incorporate your business needs and functions with your security policy and standards. A good security policy should cover physical security requirements and data security requirements for your company. You will find that a comprehensive security policy will recognize many of the identified, or unidentified, business functionalities needed for your embedded system, i.e., how the system will be used, by who, from where, types of information involved, etc.

Windows XPe Security Features

Windows XPe supports the same configurable security options as Microsoft Windows XP Professional. Let's review a summary of the security features that XPe offers and the components that need to be included during the build process.

Authentication

You need to determine if users need to authenticate to your system and or application. Is your XPe device going to be part of a domain or will local authentication be

used? XPe includes all of the Windows XP Pro authentication security components. The following tables shows the authentication features of XPe and the components needed to support them.

If you have an application that relies on the Win32 API, you must build your configuration based on Minlogon or Winlogon. XPe supports three baseline configurations:

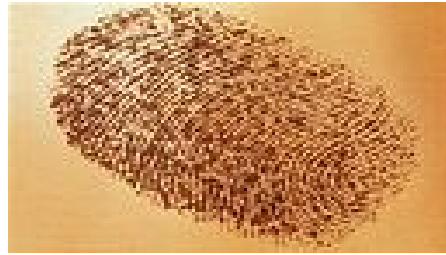
- Kernel – includes the Windows XP kernel, its dependencies, and device drivers. This configuration does not support the Win32 API.
- Minlogon – includes full Win32 API support, which allows applications to link to the Kernel32, GDI32, User32, and Advapi32 libraries. Use this configuration if your application does not require the user to log on to the system using a local or domain account.
- Winlogon – includes the standard logon process (GINA). Winlogon requires the SCM and LSASS components.

Feature	Required Components
Common Binaries	Local Security Authority Subsystem (LSASS) Primitive: Secur32 Primitive: Crypt32 Primitive: Cryptdll Primitive: Netapi32 Netlogon/NetJoin
Basic Authentication	Win32 API
Digest	Digest Authentication Security Package
Windows NT LAN Manager	Local Security Authority Subsystem (LSASS)
Kerberos	Local Security Authority Subsystem (LSASS)
Passport	Wininet Library
Credential Manager	Credential Management User Interface Key Manager Win32 API - Advanced
Secure Channel (X.059 Cert)	Local Security Authority Subsystem (LSASS) Cryptographic Network Services
Smart Card Subsystem	Smart Card Subsystem

Windows XP Embedded Security, Pt 1 By: Travis L. Schack

Authorization

Once a person or application has been authenticated, you must determine what access rights it will have on the system. How will authorization be controlled? By a local policy or a group policy? Does your security policy require auditing of events on a system? If it doesn't, consider enabling logging! Here is a table with XPe authentication features and the components needed to support them.



Feature	Required Components
Access Control Lists (ACL)	Local Security Authority Subsystem (LSASS) Primitive: NTdll
Group Policies	Primitive: AuthZ Group Policy Client Core
Local & Roaming Profiles	Primitive: profmap Local Profile Core Roaming Profile
Auditing	Local Security Authority Subsystem (LSASS) Primitive: NTdll Auditing Resource DLLs Event Log



Encryption

Your XPe device might store, transmit or process sensitive information. A developer must know what information is rated sensitive in their company and must protect the information in accordance to their company and/or customer security policy. The secure API components allow your applications to call security methods used for cryptography. The following table shows the secure API features and the components needed to support them.

Feature	Required Components
Crypto API	Primitive: Crypt32 Cryptographic Network Services

Editor's Note: Travis' article will be continued in our next issue, Fall 2004.

Travis L. Schack, CISSP, CCNA, is the President of Vitalisec, Inc.

Contact him at travis@vitalisec.com.