

the security journal

“Common Sense Security for Common Businesses”

**Expand Your Experience
Through Education!**



Our 1 year Anniversary Issue!



Security Horizon

Security Horizon, Inc.
5265 N. Academy Blvd.
Suite 1400
Colorado Springs, CO
80918

<http://www.securityhorizon.com>

Editor in Chief: Russ Rogers
Contributing Authors:

Russ Rogers, Security Horizon
Greg Miles, Security Horizon
Ted Dykstra, Security Horizon
Stephen Northcutt, SANS
Chet Hosmer, Wetstone Tech.
Chuck Menk, ESI

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.

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

Security Horizon, Inc. was founded in 2000 and is based out of 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

Your Widgets Will Not Save You!

By Stephen Northcutt.....p.7

Applying Hostile Content Detection to Digital Forensic Investigation

By Chet Hosmer.....p.9

Physical Security - Getting the Middle Child Treatment?

By Ted Dykstra.....p.14

Information Assurance in the 21st Century: It's all about the journey!

By Chuck Menk.....p.17

NSA IAM Course Schedule

.....p.19

Incident Response Part 3: Containment

By Greg Miles.....p.20

All content used by permission or Copyright 2000-2003, Security Horizon, Inc.

Notes From the Editor



Russ Rogers, CISSP, CISM
Managing Editor

There can be no doubt in anyone's mind that the computer industry continues to grow and expand at an incredible rate. New technology in hardware and software makes conducting business easier for companies in all parts of the globe. But have you ever stopped to consider the impact that these changes have on the very people that maintain your networks and ensure the security of the information that's truly critical to your organization?

This special anniversary issue of the Journal is dedicated to those security professionals out there in the world that face the seemingly insurmountable task of securing a network infrastructure that is constantly growing and changing. They're the individuals who put their head on the chopping block and they're also the ones that need sufficient management support to adequately perform their jobs.

One of the responsibilities managers have for their technical employees is continued education in new technologies. Whether the employee works strictly on the administration side of the network or is responsible for securing the network, continued funding of educational opportunities for each employee should be ensured if your business truly wants to stay on top of the ball.

There are a couple of other concerns I have for this quarter's edition as well. The first being the irrevocable damage that some security vendors have caused customers by creating an inherently flawed dependence on products to

solve their security woes. As much as many people would like to believe it, products, in and of themselves can not provide a complete security solution. That's not to say they're not useful when implemented correctly, but I suppose that's the trick isn't it? When was the last time a security vendor actually helped you identify your most critical information resources and THEN identified the appropriate solution for your organization? It's become such a numbers game to many vendors that the core concepts and concerns have been lost to create better profit margins for the investors.

My second concern is the overwhelming lethargy of thought processes concerning security that has taken hold in the business world. Granted, most companies at this point are more aware than ever before about the popular security concerns such as viruses, worms, or defaced websites, but when was the last time you considered other opportunities for compromise?

Steganography has been one of the most used tools to bypass security for numerous centuries, yet we've somehow lost touch with some of these basic concepts. Are you watching your website for information leakage? Would you even know what to look for?

In an age where the world is more focused on terrorism, deception, and misinformation than ever before; we've left ourselves strangely vulnerable. So this issue is dedicated to continued learning and education, staying on top of that ball, and using the lessons we've learned from history to keep ourselves safe.

Continued prosperity.

-Russ

SANS INSTITUTE

Setting the standard for WORLD CLASS SECURITY TRAINING

Conference Schedule November 2003 - April 2004

	SANS Security Essentials and the 10 Domains Track 1	Firewalls, Perimeter Protection, and VPNs Track 2	Intrusion Detection In-Depth Track 3	Hacker Techniques, Exploits, & Incident Handling Track 4	Securing Windows Track 5	Securing Unix Track 6	Auditing Networks, Perimeters & Systems Track 7	System Forensics, Investigation, & Response Track 8	Security +5™ Track 9	IT Security Audit Essentials Track 10	SANS 17799 Security and Audit Framework Track 11	SANS Security Leadership for Managers Track 12	Vendor Expo
SANS Network Security 2003 New Orleans, LA Nov. 14-19, 2003													V
SANS Phoenix Retreat Phoenix, AZ Dec. 1-6, 2003													
SANS NIAL VI Washington, D.C. Dec. 4-5, 2003	A special event for Managers and Leaders												
SANS Cyber Defense Initiative Washington, DC Dec. 8-13, 2003													V
SANS Biscayne Bay 2004 Miami, FL Jan. 12-17, 2004													
SANS Darling Harbour 2004 Sydney, Australia Jan. 12-17, 2004													
SANS CDI West 2004 San Diego, CA Jan. 26-31, 2004													V
SANS NIAL VII San Diego, CA Feb. 2, 2004	A special event for Managers and Leaders												
SANS Peachtree 2004 Atlanta, GA Feb. 9-14, 2004													
SANS Leadership Kauai 2004 Kauai, HI Feb. 10-13, 2004													
SANS Tysons Corner 2004 Tyson's Corner, VA Feb. 23-28, 2004													
SANS North Pacific 2004 Portland, OR March 3-8, 2004													
SANS Silicon Valley 2004 San Jose, CA March 15-20, 2004													
SANS Aloha 2004 Honolulu, HI March 21-26, 2004													
SANS 2004 Orlando, FL April 2-7, 2004 Walt Disney World Dolphin													V
SANS Online Training	●	●	●	●	●	●			●				
Instructor Led Online Training	●			●			●						
Local Mentor/Instructor Program	●	●											
Onsite Training	●											●	
Awareness Training	SANS Security Awareness Program												
GIAC Prep Teaching Kits and Practice Tests									●				

Hands-on Training
V Vendor Exposition

In today's expanding cyberworld, we're trying to save ourselves with widgets. We're installing different types of firewalls, a NIDS, many HIDS, a VPN concentrator, load balancer, attack mitigator, various new and improved antivirus detection and removal software, cryptography for files at rest and an enterprise security console to tie them all together! We continue to implement more and more widget solutions only to find ourselves bombarded with new daily hack attempts, increasingly nasty viruses, enhanced malicious worms, and it makes us wonder, "Why aren't my widgets working?"

Unfortunately, part of the reason we face this growing challenge resides with our operating system vendors. They continue to ship inferior products that have to be defended from something as simple as a packet.

In the past year, we've been hit with WebDav, SQL Slammer, Blaster, and SoBig, just to mention a few incidents. Each of these was a major event, but they should have been a non-event. If all computers had been patched and regularly maintained on a consistent basis, it would have been OK. However, that is not the case, and it is important to realize that if one of these worms had been launched with a malicious payload, the damages would have been beyond measurement.

We keep adding new software and hardware components to our systems in an effort to combat the ever-rising security concerns. However, with each new widget we install, we are adding to the complexity of our systems, creating more problems, increased aggravation, not to mention amplified costs. How many times have we installed a new component only to find it causes a conflict with another element on our system? Factor in the unnecessary troubleshooting time and resources we expend trying to figure out this

new problem on our already poorly configured system. Talk about a vicious cycle that we need to break!

It doesn't take a rocket scientist to see that complexity is its own reward; no organization has a chance of keeping a string and bailing wire facility secure, much less seamlessly working. As a rule of thumb, it's a bad sign when your perimeter is more complex than the space shuttle! That is why the Gartner approach of using an intrusion prevention system and forgetting the rest is seductive; you have a perimeter you can conceptually understand.

Of course, we need antivirus on our boxes and you can bet that if I am traveling with a laptop, it has a personal firewall. The problem here is the level of emphasis on widgets and the belief system that they will "save us." Widgets are not bad; they just don't provide airtight security. We have turned our attention to prescribed remedies that alleviate symptoms, but do not fix inherent problems. Therefore, overall security does not improve.

Talk about a vicious cycle that we need to break!

We need to understand that widgets cannot compensate for poorly patched systems. For example: an unpatched security widget itself, e.g., a firewall that has not been properly updated and patched in over a year. If you do not consistently patch your systems and an attack gets through your firewall — via a floppy, CD, or an open port — the attack can do incredible harm. We are now being told, we must update and configure our firewalls to perform deep packet inspections at wire speeds and that we need to apply security

policies based on application content as well as source, destination and port, to effectively block cyberattacks. That sounds great, sign me up! However, sadly, from all of the research I have done, the technology to do this — simply does not yet exist.

We compound the problem of fragile, unpatched operating systems with inconsistent and inferior operational practice. Over the past few years due to downsizing, many companies have elected to utilize outside developers to maintain their production servers. Too much of the critical knowledge on how things “really work” lives in too few “very busy” minds, that usually don’t have time to document what they know.

In addition, as we continue to pursue a widget-based approach towards security, we’re finding our frustration levels as well as costs — going up. Time spent troubleshooting is an indicator of how well your IT shop is run. Up to 80% of problem resolution time is spent determining the exact location and nature of the problem. Troubleshooting consumes so much time usually there is little or no accurate documentation of existing systems which leads back to inferior operational practice.



Let’s discuss a lifestyle choice as an alternative to a widget-based approach to information security. The goal here is to help each of us learn how we can improve our operations and therefore our security. If we adopt these basic concepts — change detection and management, sound operational practice,

change control, and rollback — then we can and will achieve our goal.

So, what is the best roadmap to improving overall security? A good place to begin: change detection. Invest in a little engineering first, before you move towards implementation. In other words, begin by patching and updating the “widgets”, you have. Instead of ordering a new gadget, connecting it to the network and hoping it works, do your homework. This means adopting a minimalist lifestyle; never buy a piece of hardware or software unless you absolutely need it, since you are going to have to support it.

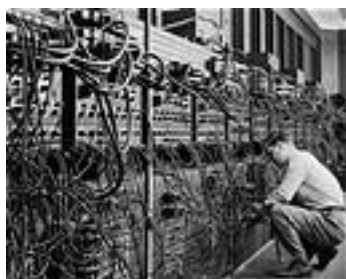
“So, what is the best roadmap to improving overall security?”

Next, check your computers for uniformity. Are they identically configured with some errors or are each of your computers unique? Personally, I would rather have identically configured boxes, in which it is easier to track down an error, than a group of unique systems. You might want to investigate how many of your systems are unique! The strategic element here is to uniformly configure your systems in a consistent manner and document the new configuration.

Sound operational practice essentially comes down to building a uniform system, installing regular updates, implementing mandatory maintenance procedures. If you create consistency, you can build in maintenance and support procedures, which is the next step. If you don’t build in proper maintenance and frequent updates, troubleshooting time is essentially unbounded.

In addition, we need to track troubleshooting time by asking technical folks to document “unplanned” work. Our goal needs to be a culture where 100% of our work is planned work. The number one key to doing this is change management. If we can detect change, rapidly determine the reason for the change, rollback the change if it is not authorized and soundly recalibrate the individual responsible for unauthorized change, we will gain far more security and endure far less cost than an IPW widget.

Finally, if we implement change control and are able to restrict the scope of our data centers to the minimum number of architectures, rollback becomes possible. At that point, we almost never have to troubleshoot. If a box behaves badly, burn it to the ground and reload it from a gold master. If it continues to behave badly, send it back to engineering to be rebuilt from scratch.



Change detection and management, sound operational practice, change control, and rollback, as a lifestyle choice, will save you money; increase your efficiency as well as security. However, this is not to say that we can get along without technology such as firewalls and intrusion detection systems, as these widgets are important tools. All we are advocating is that we treat widgets like parachutes, not airplanes!

Stephen Northcutt is a graduate of Mary Washington College. He is the author of *Incident Handling Step by Step* and *Intrusion Detection Shadow Style*, both published by the SANS Institute. He was the original developer of the Shadow intrusion detection system and served as the leader of the Department of Defense’s Shadow Intrusion Detection Team for two years.



Gargoyle™

*Hunting down
hostile content*

Do you suspect the use of password cracking programs?

Maybe you're looking for Trojan Horse toolkits?

How about encryption or steganography software?

Set Gargoyle loose on a suspect computer and find....

Steganography Tools
Key Loggers
Surveillance Tools
Trojan Horse Toolkits
Encryption Software
Password Crackers

**...even if the filenames have been changed – or the
incriminating programs have been removed.**

Applying Hostile Content Detection to Digital Forensic Investigation

By Chet Hosmer

Known File Filtering (KFF) has become a common practice during digital forensic investigations. The purpose of KFF has traditionally been to exclude files from the investigation that are “known” in order to reduce the amount of digital information that needs to be examined. The process of doing so is quite simple. First, the investigator must generate a one-way digital hash (see description to the right) for each file that is extracted from the suspect media (hard drives, CD’s, DVD’s, thumb drives, etc.) and compare that digest to a database of known file hashes. If the file is known, the investigator marks the

One-Way Digital Hash

“One way hash algorithms (such as MD2, MD4, MD5 and SHA-1) take arbitrary length input and generate a fixed length hash-value or hash code. The basic idea is that a hash-value serves as a compact representation of an input string. To be of cryptographic use, a hash function h is typically chosen such that it is computationally infeasible to find two distinct inputs which hash to a common value (i.e. a collision).” *Handbook of Applied Cryptography*, 1997 CRC Press

file as such and can safely ignore it during the investigation and focus attention on the files created or modified by the suspect. Several databases of hash codes exist for this purpose. Most notably, the National Institute of Justice (NIJ) and National Institute of Standards and Technology (NIST) have created the National Software Reference Library (NSRL). The NSRL provides a repository of known software, file profiles, and file signatures for use by law enforcement organizations in computer forensic investigations. This reference library is critical to the advancement of digital forensic investigation methods. It offers a trusted standard – one of the first of its kind in the digital forensic arena



Figure 1: National Software Reference Library

Photo Courtesy of NIST

Today, more than ever, methods and techniques are needed to reduce the time of investigations as case loads expand and resources become stretched to the breaking point. “Currently, submission rates for digital evidence laboratories are growing between 20 and 60 percent per year, and examination backlogs are typically averaging between 2 and 9 months! Even the most limited computer examinations take 3 to 5 days, and in-depth analyses can take 2 to 3 weeks. When compared to most other forensic sciences, digital evidence is a high-pressure and labor-intensive endeavor, with significant operational issues (backlogs, turnaround times, mission creep, etc.) and critical infrastructure problems (lack of examiners, lack of space, continuous need for updated software and hardware, etc.). Alternative solutions such as automation or intelligent software do not appear to offer much promise, at least in the near term.”¹

¹ <http://www.usdoj.gov/dea/programs/forensicsci/microgram/mg0603/mg0603.html>

“Not surprisingly, this situation is highly frustrating for management and budget planners. From their perspective, digital evidence programs represent a serious “problem” that

(much more often than not) is getting ever worse despite the ever-increasing input of additional resources. And there’s seemingly no end in sight.”¹

¹ <http://www.usdoj.gov/dea/programs/forensicsci/microgram/mg0603/mg0603.html>

Figure 2: Hard Drive Size by PC Type¹

¹ <http://www.pcpitstop.com/research/HDD.asp>

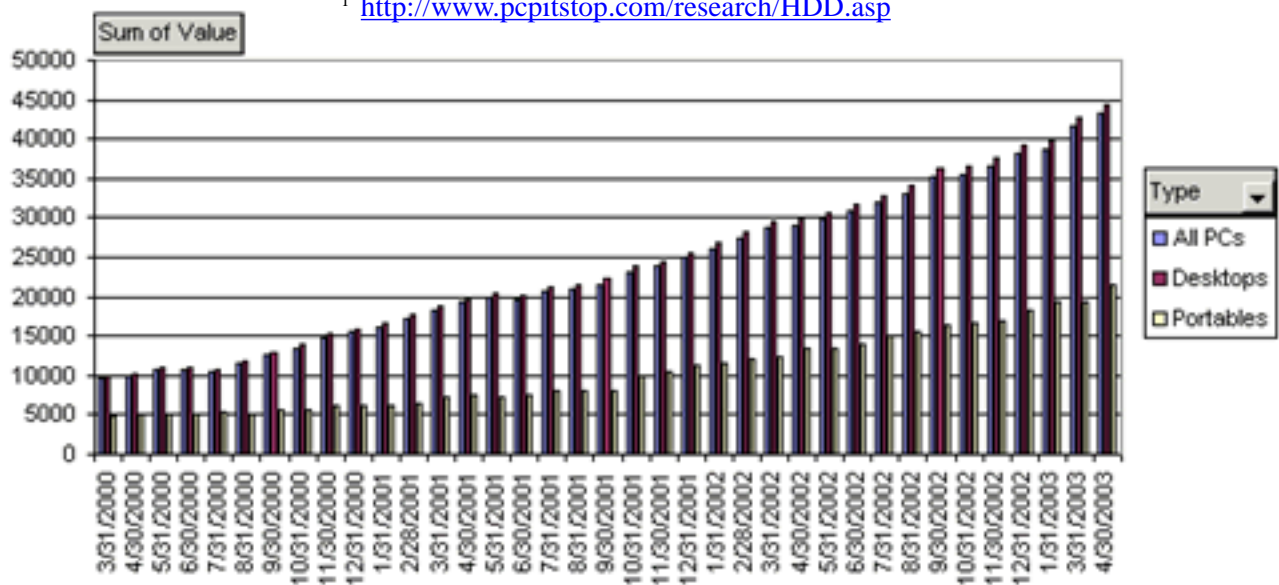
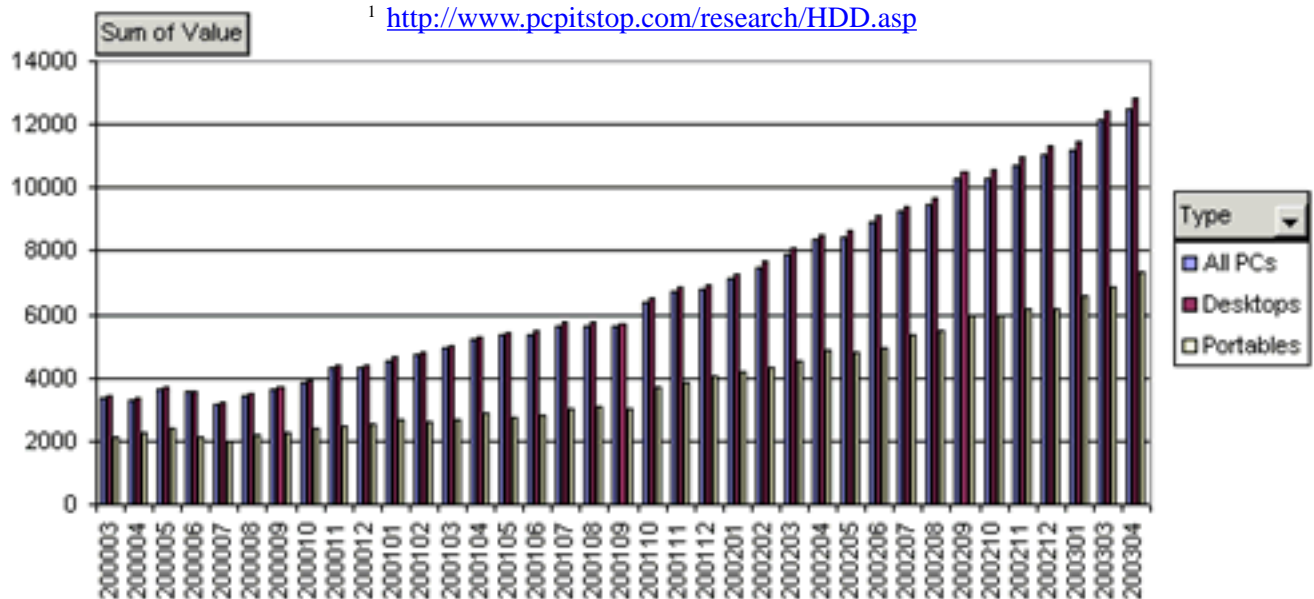


Figure 3: Used Drive Space by PC Type¹

¹ <http://www.pcpitstop.com/research/HDD.asp>



Digital hash methods again can offer significant assistance in the rapid examination of both suspect and victim drives and media. We have recently developed our own method based on this practice, called "hostile content detection". It borrows some of the principles from KFF but applies them in a fresh way. Hostile content detection allows investigators to employ datasets like NSRL or build their own specialized databases of hostile or malicious hash codes, which can provide significant clues regarding the activities, motives, and even the intent of suspects or potential suspects – and the process can be performed in just minutes. Speed and accuracy are the obvious objectives of such a process; however, an added benefit is the automatic generation of new clues and information, not just additional data.

One of the interesting aspects of hostile content detection is the generation of the databases of the hash codes themselves:

1. In many cases, hostile content needs to be obtained from hackers, crackers, hacked systems, ongoing or historical investigations.
2. The hostile content needs to be inventoried and a digital hash must be generated for each file associated with the hostile content. It is important to remember that hostile content can be virtually any digital file. The most common is software such as steganography programs, encryption software, password crackers, virus and hacking toolkits, etc. However, it can also be files attached to e-mails that were exchanged by accomplices, child pornography images, audio and video files. Any digital file that can help identify illegal or hostile activity, intent, methods etc., can be cataloged. This process requires special care and a quarantined

3. Finally, these malicious applications and contraband tend to evolve rapidly because in many cases, source code is available. The modifications that generate differing strains are rapidly released, requiring the digest databases to be constantly updated.

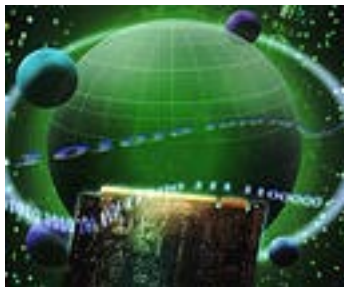
The first step in generating such a database is to identify and categorize the types or kinds of hostile datasets to catalog. To date, we have identified the following categories:

Data Hiding (Steganography)
Encryption Programs
Hacking Tools
Cyber Surveillance Tools
Trojan Programs
Password Cracking Tools
Virus Building Toolkits
Wired Surveillance Tools
Wireless Surveillance Tools
Denial of Service Tools and Toolkits
Spy ware
War driving and dialing tools

Once the categories have been identified, the initial collection process begins as mentioned above. This process must be ongoing as new versions or strains are identified. The arduous process of installing each cyber weapon on a clean system to identify all the files and remnants is then accomplished. Once all the digital files are identified, a digest is created and the files are archived. Next, the database is updated and the files are associated with their source and category. The linkage here is critical so not only can we identify a potentially hostile file, but also be able to associate it back to the source and category. To illustrate; if we positively identify the file *zlib.dll* on the suspect system, this information alone is not very useful without context. Associating this file with the installation of S-Tools allows us to identify the source program. So then,

what is S-Tools? It is a well-known steganography program that can be used to hide incriminating information in digital carriers (image and audio files). Specifically, S-Tools is able to hide information inside BMP and GIF images as well as audio WAV files. This simple detection has allowed us to deduce the following:

1. At some point in time, the suspect has installed a steganography (data hiding) program on their computer. This may indicate that the suspect at least intended on hiding information in a covert fashion.
2. This should immediately raise the level of sophistication that we associate with this suspect, since steganography is a fairly esoteric cyber weapon.
3. We should investigate and examine the BMP, GIF, and WAV files on the suspect's computer a bit more closely in order to potentially identify whether data hiding was actually attempted by the suspect.
4. We also should question the suspect as to his or her intent or use of such a program.



We must seriously advance technologies that provide highly qualified information, not simply a set of regurgitated data. We must continue to develop tools and technologies for those on the front lines, which can be easily adapted to the present situation, mission and domain specific threats.

The progression of methods and the acceleration of techniques for rapidly detecting and identifying potentially hostile content for the purpose of assessing the activities, behaviors, and interests of criminals and/or terrorists are at a critical stage. Without the immediate evolution of tools, techniques, and methods for performing advanced search, seizure, analysis and profiling; criminals and terrorists will continue to utilize and advance cyber weapons and techniques. In 1960, Attorney General Robert Kennedy stated the following, "If we do not, on a national scale, attack organized criminals with weapons and techniques as effective as their own, they will destroy us." Unfortunately, this statement is as relevant today as it was back then.

Chet Hosmer is a co-founder, and the President and CEO of WetStone Technologies, Inc. His specialty areas include secure time, intrusion detection and response, and cyber forensics.

If you'd like to contact Mr. Hosmer, you may reach him at chet@wetstonetech.com

Black Hat[®] 2004 Windows Security



Call for Papers

Submissions are currently being accepted for the upcoming
Black Hat Windows Security 2004 Briefings.

For more information and to submit, please go to www.blackhat.com



Physical Security:

Getting the Middle Child Treatment?

By Ted Dykstra

The tragic events of September 11, 2001 brought physical security to the top of the priority list. But parallel with the Birth Order Theory (BOT), physical security quickly returned to its normally appreciated status, that of being the middle child in all its ignored glory. This security kid pervades every aspect of IT security, yet is under-appreciated and often overlooked, as the CXO-Parent's attention is monopolized by the other siblings.

The oldest child in this imaginary trio of security kids would be your system level components. When born, or implemented, these components dominate attention, and a great deal of thought and consideration is put into each and every step of their development. As they get older they mature, become more reliable and dependable, and then whammo. In an attempt to regain your attention they open your boxes up to a newly discovered flaw. Then of course there's the baby of the security family. The bleeding edge security controls that spend your investments with so much ease, because you just can't say no to them. You spend so much time tweaking and fine-tuning it as well, that there's really very little attention left for you to give to the others.

I must admit that I too have ignored aspects of physical security following the BOT, just because there were always "more important" issues to deal with. Like implementing Dr. Spock's (insert your vendor) latest patch release, or "playing" with some new technologies. A wake-up call came this summer when I had the opportunity to witness a lock-picking contest at the DEFCON 11 security gathering in Las Vegas, Nevada (<http://www.defcon.org>). If you're not a physical security expert, the results of an event like this might surprise you. Most of the locks used in the contest were standard residential units available at any hardware store across the

country. The chilling part is that some contestants were picking these locks in less than ten seconds! The best single lock score was just around six seconds.



To be honest, I was flat out amazed; actually, I was in awe. I was also surprised by the diversity of the contestants. There was a wide array of "professionals" and "hobbyists" (or at least that's my understanding), of disparate ages and backgrounds. In fact, the winner looked like he may not have been old enough to drink. In talking with him, I found out that he had begun this "sport" only a few months prior. He had made his only picks out of street sweeper brushes! So, with homemade lock-picks and a few months of practice, he jumped at the chance to compete against roughly forty others at the annual "security party." Incredibly, he won 1st place by picking a deadbolt, doorknob, and padlock in the final round in approximately two and a half minutes. I had "dabbled" myself previously, but this was truly an awakening for me. It was then that I realized I had been ignoring a major aspect of information security.

It's true that as information security workers, we realize that physical access to devices pretty much negates any and all controls that we may have implemented. We understand that once console access has been achieved, that pretty blinking firewall is not solely capable of protecting us. The problem is that we already juggle multiple aspects of knowl

knowledge we must keep fresh in order to perform our duties. Multiple OS and application commands, vulnerabilities, and patches. Multiple firewall vendor commands, versions, capabilities, and implementations. Multiple IDS abilities, configurations, best practice architectures, and reported anomalies. Multiple detection tools usage, false positives, dangerous checks, and “tips & tricks.” Undoubtedly, you can think of many more to throw on top of that. I began to specialize in security years ago for two reasons: the sheer joy of breaking something (did I say that?), and the opportunity to “specialize.” The first reason still applies, but the term specialty seems to have lost it’s meaning over the years. Physical security, among other things, just wasn’t on my list when I began my forays into subverting the evil hacker types!

As far as attention goes, physical security is still treated like the middle child. It seems as though many IT managers approach it with a “fire and forget” mentality, installing some fancy proximity badges or key card access points and relying on standard door locks as well. Now that a physical security perimeter has been defined and implemented, who’s watching? The ROI (the key to selling anything commercially these days) of these automated systems over manned security patrols is undeniable. At least in the event that nothing ever happens. Even if a CCTV system is implemented, how many of those have rotational tape or digital storage that is never reviewed until there is a discovered incident? How often do most organizations review logs from their badge servers? How often does someone approach their middle child and inquire about the their day? Organizations are becoming much more aware of the need for security assessments and audits to determine the efficiency of their controls, but physical security audits continue to be a rare breed and are overshadowed by the

attention afforded to its other siblings.



One parting thing to think about, the quietest and yet most abundant topic of discussion I’ve been involved in as of late, has been the method for beating proximity badge readers. I’ve spoken with several different computer “clubs” working on these projects. I’m by no means an expert on the subject, but this could have rather dark implications. It would make a physical break in as simple as associating to an unencrypted wifi network with a non-broadcast ESSID.

This discussion was meant to light-heartedly share a security concern that too many people appear to have ignored over the years, myself being one of them. Especially those customers spending too much time with the baby! Try not to fall into the BOT trap too often! And yes, I have two siblings myself, but I’ll let you guess which one I am!

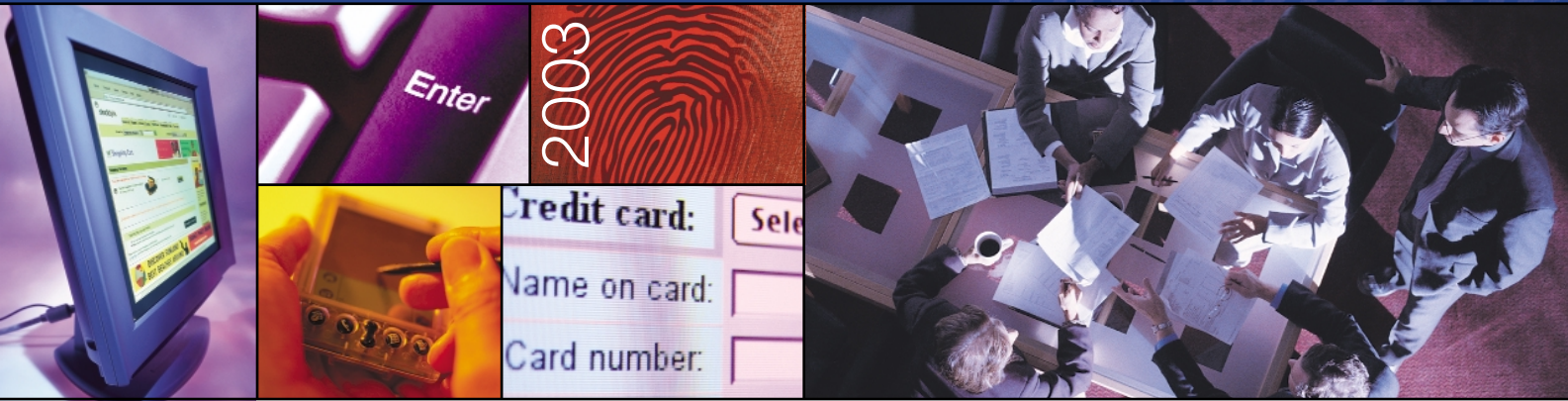
Ted Dykstra, CISSP, CCNP is a security consultant at Security Horizon and regular contributor to The Security Journal.

If you’d like to contact Mr. Dykstra, you may reach him at the following:

ted@securityhorizon.com,
www.securityhorizon.com
719-488-4500.

FREE
EXHIBIT HALL
ADMISSION
Register
online

Security is more than an IT issue.



It's everyone's business.

Today, information security is a shared responsibility, top-of-the-agenda in the board room as well as the server room. Smart business executives understand security is more than technology—it's *business* policy, process, procedure and ultimately, *business* advantage. And smart IT pros understand that the right security starts with making the right *business* case for it.

That's why Infosecurity 2003 will be held in New York—the business capital of North America. For information asset stakeholders, the Infosecurity Conference & Exhibition is the ideal forum to share real-world concerns and discover the most promising new security solutions.

Make plans today to attend Infosecurity 2003 in New York.

Attend
infosecurity

2003

Register or learn more at
www.infosecurityevent.com

Conference: December 8–11, 2003
Exhibition: December 10–11, 2003
Jacob K. Javits Convention Center
New York, New York
www.infosecurityevent.com

To register online and for event updates, visit our websites. Or call 888.251.0566 or 203.840.5690. For information about exhibiting, please contact Mike Alessie at 1.203.840.5387.

Produced by:

 Reed Exhibitions

 ISSA™

**INFORMATION
SECURITY**

Information Assurance in the 21st Century: It's all about the journey!

By Chuck Menk

In the rapidly changing Information Assurance (IA) landscape of the 21st century, the best assessment, vulnerability analysis or penetration test does not seem to be “good enough”. What is needed are IA professionals embedded in well-defined organizational structures designed to battle the threat on a day to day basis. This does not devalue the need for expert assessors, vulnerability analysts and penetration testers. In fact, it helps to focus their skills by ensuring they are used in the most cost effective and efficient manner. In addition to traditional Information Security (INFOSEC), Computer Security (COMPUSEC) and Vulnerability Analysis (VA) techniques, the IA arsenal of today requires tools to measure organizational capabilities. We need to address the seemingly overlooked security issues arising from the systemic failure to provide adequate process capabilities and a robust working environment to support and maintain the technical experts in the field.

In the early 1990s, while working in support of the National Security Agency's (NSA) Trusted Product Evaluations Program (TPEP), it became painfully apparent that the issue with evaluating COMPUSEC solutions was not so much the lack of skilled security engineers (believe me I have worked with some of the best), so much as the lack of infrastructure to support them in the development life cycle. I can not recall a single evaluation team that raved over the completeness or accuracy of the system development artifacts required to prove the secure production of the product under evaluation. As a result, the evaluators spent most of their time helping to “develop” the needed artifacts before they could conduct a reliable evaluation. Eventually the cost of the program (in time) to the participating vendors and government evaluation teams reduced the players to a handful of firms and

sparked the development of a “faster and better” program that eventually lead to the Common Criteria Evaluation and Validation Scheme (CCEVS).



About the same time, a movement within the Capability Maturity Model (CMM) world to create a System Security Engineering approach (SSE-CMM) had begun in an attempt to build security engineering into the overall System Engineering process. In 1995, a group of commercial companies and government agencies shifted their focus to this activity with the belief that building in security from day one would help fellow security professionals to focus on their core concerns (e.g. performing COMPUSEC evaluations, VAs and conducting penetration testing) and help vendors deliver more reliable, secure, and cost effective solutions in a timely fashion. Involvement in this activity opened many eyes to the general lack of security infrastructure even within some of our most treasured security agencies and commercial System Security Engineering providers. From 1995 to 2002 the SSE-CMM was developed, piloted, fielded and accepted as an ISO standard.

In 1999 a variant, the INFOSEC Assurance CMM (IA-CMM), previously the INFOSEC Assessment CMM, was created to support the NSA's INFOSEC Assurance Training and Rating Program (IATRP), previously the

INFOSEC Assessment Training and Rating Program. It is this variant of the SSE-CMM that carries the greatest potential for enhancing and growing general awareness within the 21st century IA landscape with the added benefit of providing support for the ever growing set of homeland security concerns.



As the IA-CMM was developed, piloted and fielded from 1999 to the Present, it became apparent that its worth reached beyond the bounds of its original purpose. The model was originally developed to measure the maturity (i.e. robustness) of a company's INFOSEC assessment capabilities. The NSA needed to bring more talent to the assessment arena to relieve the backlog of DoD customers requesting these services. The IATRP became the vehicle to achieve this end. While the intent of the IA-CMM was to provide relief to DoD INFOSEC assessment needs, a subset of the seven currently rated organizations quickly realized the merits it brings to non-DoD IA customers (e.g. Commercial IA, HIPPA compliance activities, and the Financial industry). In addition, firms trying to determine their own internal IA capabilities have started to request IA-CMM training and self-assessment support. They have embraced the IA-CMM as a means of building internal IA awareness so they can determine when and where to apply the focused analysis attained from professional IA assessors, vulnerability analysts and penetration testers.

Prior to using a tool like the IA-CMM, organizations would generally ask for help after they have been attacked or at random intervals in

an attempt to find the holes and "fill them". But, without a resident knowledge, management support and adequate funding of IA processes, how long could one expect the holes to remain filled or how certain can they be that new ones are not developing? IA professionals in isolation can only do so much. For many firms, it is becoming obvious that there is a need to develop an internal capability to oversee their IA requirements. In preparing for an IA-CMM appraisal, organizations learn the fundamentals of good IA process and strengthen organizational support. The byproduct is a competent self-assessment capability that can identify areas of critical concern and help the IA assessors, vulnerability analysts and penetration testers to build a diversified IA security posture.

“Gone are the days of the ‘super hero’ IA professional.”

In the dynamic IA landscape of the 21st century and beyond, we need to build IA teams embedded in our organizations to deal with the day to day threats to our infrastructure. Gone are the days of the “super hero” IA professional. The complexity of the security problem and sheer volume of information being transmitted today calls for teams of specialized experts working together to succeed in defending against the onslaught of threats in the modern age. Tools like the IA-CMM can make all the difference in identifying and maturing these capabilities. Now is the time for organizations to work together to determine what they need to protect themselves from potential exploitation. Due to the open access across firms, the failure of one can lead to the collapse of another. Internal IA capabilities need to be in place to identify when and where to

call in the professional IA assessors, vulnerability analysts and penetration testers and address their findings as part of an ongoing set of IA processes and procedures. We all need to work together to succeed!



Charles G. Menk III, CISSP¹
*Director, Information Assurance Programs
Engineering Solutions, Inc (ESi)*
Phone: 410-694-0700 x104
Fax: 410-694-0780
Pager: 800-709-6502
Web: <http://www.enginsol.com>

¹ The views and discussions presented in this article are those of the author and may not be representative of ESi.



10/13-10/14, 2003	Atlanta, GA
10/20-10/21, 2003	Denver, CO
10/27-10/28, 2003	Phoenix, AZ
11/3-11/4, 2003	San Diego, CA
11/6-11/7, 2003	Philadelphia, PA
11/6-11/7, 2003	Washington DC
12/8-12/9, 2003	New York, NY
	Infosecurity 2003
2/27-2/28, 2004	Seattle, WA
	BlackHat Windows
6/4-6/5, 2004	Myrtle Beach, SC
	TechnoSecurity
7/26-7/27, 2004	Las Vegas, NV
	BlackHat USA

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** training.

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

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



Last issue we took a look at the critical, difficult step of identifying a computer security incident. This article is the third 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), CanCERT™ in Canada (cancert.ca), and the Forum for Incident Response Security Teams (FIRST) (www.first.org). This article focuses on IR Containment.



The primary goal of the Incident Response Team is to maintain/restore business continuity, so containment of a security incident is vital. The purpose of containment is to limit the extent of an attack. The key elements of containment are decision-making and carrying out some predetermined steps. The decision process defines the critical steps that will be taken. Decisions have to be based on the business needs of the organization, criticality and value of the information/system involved, and regulatory/legislative requirements or the industry the organization is involved.

The decisions may include:

- Shutting down a system
- Disconnecting a system from the network
- Monitoring system or network activity (network surveillance)
- Calling in Law Enforcement
- Setting traps to allow for further investigation
- Disabling certain functions (telnet, ftp, other bad ports, etc)

Keep in mind that by removing access, you provide yourself “denial-of-service” and you also notify all users of the incident including potentially the person causing the problem. In some cases, removing all access or functionality may be warranted, then restore normal operation in limited stages. In some cases, it is worthwhile to risk some damage to the system if keeping the system up might enable you to identify an intruder.

It is critical during the containment stage to follow a predetermined set of procedures. Your organization or site should, for example, define acceptable risks in dealing with an incident, and should prescribe specific actions and strategies accordingly. This provides the opportunity for quick decisions to be made when needed. In the containment stage of incident response, notification of appropriate authorities is critical.

“ It is critical during the containment stage to follow a predetermined set of procedures. ”

Steps for Containment:

- Deploy containment team
- Secure area affected so no one accidentally starts changing things
- Review information from the identification phase
- Do not allow the system to be altered until a complete backup can be taken. Ideally this is a bit for bit image of the hard drives
- Avoid looking for the attacker by obvious methods
- Maintain standard procedures
- Don't forget about "rules of evidence" and forensically protecting the evidence
- Consider planting "honey pots"
- Be cautious of compromised code (i.e. don't log in as root or administrator on a potentially compromised machine still hooked to the network)
- Backup the system to forensically sterile media
- Store media in a safe location
- Acquire and review router and system logs
- Review logs from neighboring systems, especially if there is a trust relationship
- Determine the risk of continuing operations
- Keep system owners and administrators briefed on progress
- DO NOT attempt to assign blame until the incident handling process is completed
- CHANGE PASSWORDS and enforce a strong password policy
- Call in additional expertise if needed
- Keep detailed records of every action taken during this phase• Call in additional expertise if needed
- Keep appropriate people and organizations informed throughout the

process – Communications Is Key!

It can be difficult to create a blanket set of step-by-step procedures to cover every organization because each organization and each operating system is different. Different risk factors will have to be set dependant upon the operations and function of the organization. But you can follow some basic procedures that keep you within the acceptable boundaries of action during containment. These parameters have to be set before an incident occurs, otherwise there will be disorganization and confusion while trying to contain the incident. Clearly, Preparation (see article: Incident Response Part 1: Preparation) is still the most important step in the incident response process.

Next IR article, we will be discussing Incident Response Part 4: Eradication.

Dr. Greg Miles, CISSP, CISM is the President of Security Horizon and a regular contributor to The Security Journal.

If you'd like to contact Dr. Miles, you may reach him at the following:

greg@securityhorizon.com,
www.securityhorizon.com
719-488-4500.