The Vulnerabilities of Developing on the NET

Robert A. Martin

April 2001

Published in

The April Issue of CrossTalk Magazine

CROSSTALK
The Journal of Defense Software Engineering

CVE
cve.mitre.org

The Vulnerabilities of Developing on the Net

Robert A. Martin
The MITRE Corporation

Disaster has struck. You would think that firewalls, combined with filtering routers, password protection, encryption, and disciplined use of access controls and file permissions would have been enough protection. However, an overlooked flaw in the commercial web server application allowed a hacker to use a buffer overflow attack to leverage the application's privileges into administrator-level access to the server. From there it was easy to gain access to other machines within the Intranet and replace the public Web pages with details of the hack. With the company's public site showing a live video stream of an ongoing internal, private and sensitive company meeting, it left little room for doubt as to how badly they had been hacked.

While most organizations have addressed the various aspects of implementing cyber security, many are failing to successfully address the one security area where someone can bypass all other efforts to secure the enterprise. That area is finding and fixing known security problems in the commercial software used to build the systems. There may be an answer, however, that will transform this area from a liability into a key asset in the fight to build and maintain secure systems. The answer rests in an initiative to adopt a common naming practice for describing the vulnerabilities, and the inclusion of those names within security tools and services. The initiative has been in practice for more than a year across a broad spectrum of the information security and software products community: It is called the Common Vulnerabilities and Exposures (CVE) initiative.

To Err Is Human

Every programmer knows they make mistakes when writing software, whether it be a typo, a math error, incomplete logic, or incorrect use of a function or command. Sometimes the mistake is even earlier in the development process – reflecting an oversight in the requirements guiding the design and coding of a particular function or capability of a software program. When these mistakes have security implications, those with a security bent will often refer to them as vulnerabilities and exposures.[1]

All types of software, from large complex pieces to small and focused ones, are likely to contain software mistakes with security ramifications. Large complex software like operating systems, database management systems, accounting systems, inventory management systems, as well as smaller applications like macros, applets, wizards, and servlets need to be evaluated for mistakes that can impact their security integrity. Remember that when we put these various software products together to provide an overall system, each of the software elements that make up the system could be the one that compromises it.

Things were different in the past when an organization's computer systems were stand-alone and only interacted with other systems within the same organization. Only a few systems used tapes and file passing to exchange information with outside systems. The same holds true for government and military systems, including weapons. This isolation meant that errors in commercial or developed software usually had limited impact, at least from the public's point of view. In fact, most errors, crashes, and oversights went unnoticed by the general public. At most, these problems would cause occasional troubles for an organization's closest business partners.

There Is No Hiding Now

The same is not true today. Very few of today's organizations, whether in the private sector or government, have or build self-contained systems. It is the norm for employees, customers, business partners, and the general public to have some degree of access and visibility into the minute-by-minute health and performance of an organization's software environment. Processing delay, calculation mistakes, system downtime, even response time slowdowns are noticed and often draw criticism.

Accompanying this increased visibility is an explosion in the different ways systems are accessed and used. Web and application servers have been created to help make systems interconnect and leverage Internet-based technologies. Access to web sites, purchase sites, online help systems, and software delivery sites makes the organizations that own the sites very visible. To better support business partners and employees working at remote locations, on the road, or from home, we have connected our backroom systems to the corporate Intranet and extranet. New technologies have emerged, like instant messaging, mobile code, and chat, whose functionality requires effortless access by users across organizational boundaries. The movement to highly accessible systems, driven by the need to save time and make businesses more efficient, and the reality of having to do more with less, has dramatically increased the impact of mistakes in commercial software.

While errors in self-developed software can still have a major impact on an organization's ability to function, it is the vulnerabilities and exposures in the commercial software they use to build systems that creates the bigger problem. A mistake in a commercial program can open a front or a back door into situations that most organizations strive to avoid. A mistake permitting unauthorized access can expose private information about customers and employees. It can allow hackers to change information or perform services with your systems to their own advantage. In addition, a vulnerability can allow them to shut down your internal and publicly accessed systems, sometimes, without your knowledge. In those cases where the vulnerability or exposure allows someone to make changes or bring down systems, or when the theft of services and information is eventually noticed[2], there can be a huge impact to the organization's public image[3]. There can also be legal liability and direct operational impact.

What Can You Do?

Determining the vulnerabilities and exposures embedded in commercial software systems and networks is a critical "first step" to fixing the problems. A simple patch, upgrade, or configuration change could be sufficient to eliminate even the most serious vulnerability, if you know what you need and how to get it.

To find information about vulnerabilities in commercial software that your organization uses, you have to do some research and probably spend some money. With commercial software, the customer has little or no insight into the implementation details. At the very best you may have an understanding of the general architecture and design philosophy of a package. Companies offering commercial software treat the design details and software code as business-critical private information. In addition, since most of these companies are highly competitive, commercial software vendors are sometimes reluctant to share their problems, even with their customers.

Who Knows?

So how do you find out about commercial software vulnerabilities if the vendors are not going to tell you? During the last decade, three groups have emerged who share the same curiosity. For sake of discussion we will refer to these as the hackers[4], the commercial interests, and the philanthropists. The hackers, unfortunately, want to find vulnerabilities and exposures so they can exploit them to gain access to systems.

Those with commercial interests want to be hired to find the mistakes, or they want you to buy their tools to help you find the vulnerabilities and exposures yourself. They offer their services through consultants who will evaluate your software systems, and through tools that you can buy and run yourself. Some proffer the use of their tools as an Internet-based service. This group includes software and network security companies that provide security consulting services and vulnerability assessments, databases of vulnerabilities and exposures, and the tools for security services and vulnerability evaluations.

The philanthropists include security researchers in various government, academic, and non-profit organizations, as well as unaffiliated individuals that enjoy searching for these types of mistakes, usually sharing their knowledge and tools freely.

Each group has members focused on sharing information: among like-minded hackers, for a price in most cases for the commercial interests group, and generally for free in the philanthropists group. For all three groups the search for vulnerabilities and exposures in commercial software is challenging since the commercial marketplace is constantly developing and authoring new classes of software capabilities and new ways of using them. This mushrooming of commercial software capabilities also creates an ever-changing challenge for organizations using commercial systems. The challenge is to correctly configure and integrate the offerings of various vendors without opening additional vulnerabilities and exposures from configuration and permission mistakes.

How to Find Out

In response to the arduous task of tracking and reacting to new and changing vulnerabilities and exposures, the members of these three groups are using Web sites, news groups, software and database update services, notification services like e-mail lists, and advisory bulletins to keep their constituents informed and current.

So information on vulnerabilities in commercial software is available. That is great, right? Well, not quite. There are several problems. The biggest is that each organization (or individual) in these three groups has been pursuing their vulnerability discovery and sharing efforts as if they were *the* source of information on vulnerabilities. Each uses its own approach for quantifying, naming, describing, and sharing information about the vulnerabilities that they find. Additionally, as new types of software products and networking are introduced, whole new classes of vulnerabilities and exposures have been created that require new ways of describing and categorizing them.

Another problem is that finding the vulnerabilities and exposures within systems is just the first step. What we really want to do is to take the list of vulnerabilities and get them fixed. This is the software vendors' domain – those who create and maintain our commercial products. Unless they use the same descriptions and names as the hackers, commercial interests, and philanthropists groups, it is difficult, confusing and frustrating to get the fix for any particular problem you find.

A Closer Look at Who Knows What

The Internet is the main conduit hackers use to share information on vulnerabilities and how to exploit them. Different member organizations in the commercial interests group have their own mechanisms for sharing vulnerability information. For example, the tool vendors create vulnerability scanners that are driven by their own vulnerability databases. The intrusion detection system (IDS) vendors build different types of software systems for monitoring your network and systems for attacks. There are also scanner and IDS tools available from the philanthropists group as freeware. Both the scanner and IDS providers have to continuously update their tools with new information on what and how to look for problems. Examples of these organizations and tools are shown in Table 1.

Scanners typically include tests that compare version infor-

Table 1. *Scanner and IDS Offering Examples*

Product	Tool Type	Organization
Centrax	scanner/IDS	CyberSafe
CyberCop	scanner	Network Associates
Dragon	IDS	Network Security Wizards
HackerShield	scanner	Bindview Corporation
LANPATROL	IDS	Network Security Systems
Nessus	freeware scanner	Renaud Deraison & Jordan Hrycaj
NetProwler	IDS	Axent Technologies
QualysGuard	ASP-based scanner	Qualys
RealSecure	IDS	Internet Security Systems
Retriever	scanner	Symantec Corporation
SAINT	scanner	World Wide Digital Security
Secure IDS	IDS	Cisco Systems
STAT	scanner	Harris Corporation
SWARM	scanner	Hiverworld, Inc.

mation and configuration settings of software with an internal list of vulnerability data. They may also conduct their own scripted set of probes and penetration attempts. IDS products typically look for indications of actual attack activities, many can then be mapped to the specific vulnerabilities that these attacks could exploit. The scanner market recently developed a self-service-based capability. It uses remotely hosted vulnerability scanners on the Internet that you can hire to scan your Internet resident firewalls, routers, and hosts. The results of the scans are provided through a secure link, and you can usually run the scans whenever you want. These scans are shielded from everyone but you, including the service provider. IDS capabilities are often available as part of a managed security service, where the organization contracts out the intrusion detection and monitoring to a security services vendor.

Both IDS and scanner tool providers harvest information about vulnerabilities and exposures from public information sites, hacker sites, newsletters, and advisories. They also have their own investigative researchers who continuously look for new vulnerability information that will make their company's offering better than the competition[5], as well as providing them with the "free" advertising that comes with finding and publicly reporting new vulnerabilities and exposures. Typically, these researchers serve as consultants within the company, offering their services to evaluate an organization's systems and networks. Their parent companies also offer databases of vulnerabilities for a fee, although some also share the information openly as raw information on a Web site.

Some members of the philanthropists group also offer very sophisticated search and notification services for free, but their veracity, quality, and levels of effort vary considerably. Examples of vulnerability-sharing organizations are shown in Table 2.

Site Name	Type	Organization
arachNIDS	free IDS database	Max Vision Network Security/Whitehats
CERIAS Vulnerability Database	database	CERIAS/Purdue University
Fyodor's Playhouse	hacker web site	Insecure.Org
Online Vulnerability Database	database	Ernst & Young's eSecurityOnline.com
ICAT Metabase	free web site	NIST
Bugtraq mailing list Database	mailing list database	SecurityFocus.com
PacketStorm	hacker web site	Securify, Inc.
SWAT Database	database	Axent Technologies
Vigil@nce AQL	database	Alliance Qualité Logiciel
X-Force Database	free web site	Internet Security Systems

Table 2: *Vulnerability Sharing Examples*

In addition to freeware scanner, IDS tools, and vulnerability databases, the philanthropists group's government and academic members offer several announcement, alert, and advisory services that are widely used and highly valued. Some commercial interests group companies offer these types of free services as well. Examples are shown in Table 3.

There are numerous venues for finding out what vulnerabilities and exposures exist in your organization's commercial software systems, as well as many tools and service providers willing to help you determine which vulnerabilities and exposures you have.

The three groups we've covered -- hackers, commercial interests, and philanthropists – all address locating the vulnerabilities and exposures in the commercial software that forms the base of your live systems and networks.

Service	Type	Organization
Bugtraq	e-mail list	Bugtraq
Casandra	alerts	CERIAS/Purdue University
CERT Advisories	advisory	CERT Coordination Center
CyberNotes	monthly newsletter	NIPC
Razor	advisory	Bindview Corporation
S.A.F.E.R.	monthly newsletter	The Relay Group
SANS NewsBites	e-mail list	SANS Institute
Security Alert Consensus	e-mail list	Network Computing and SANS
SecurityFocus Newsletter	newsletter summary of Bugtraq e-mails	SecurityFocus.com
SWAT Alerts	alerts	Axent Technologies
X-Force Alert	advisory	Internet Security Systems

Table 3: *Alert and Advisory Services Examples*

We will now address finding the "fixes." The product vendors who make the software in which these vulnerabilities were found provide the solutions for vulnerabilities. Many of them have their own methods of providing their customers with software fixes and updates. Until recently, most vendors were not very proactive in distributing patches and updates outside of their normal software development cycle. This has improved considerably. Now, many major vendors provide alerts and advisories concerning security problems, fixes, and updates (See Table 4).

Service	Type	Organization
IBM ERS	advisory	IBM
Microsoft Product Security Notification Service	advisory	Microsoft Corporation
SGI Security Advisory	advisory	Silicon Graphics, Inc.
Sun-alert	alert	Sun Microsystems, Inc.

Table 4: *Vendor Alert and Advisory Services Examples*

But can these various vulnerability services, tools, and databases, along with the software vendor's update announcements effectively combine to help you assess, manage, and fix your vulnerabilities and exposures? The short answer is that it used to be very difficult, but now a way to do it seems to be at hand. So what was wrong, and what changed?

The Tower of Babel

In 1998 if you tried to use these various tools, services, and databases you were faced with a problem rooted in each ones heritage. Each had developed its own naming standards and methods for defining individual entries in their respective vulnerability data stores. Table 5 shows how the same vulnerability was referred to by 12 different names by 12 leading organizations. With such confusion, it was very hard to understand what vulnerabilities were faced, and what vulnerabilities were or were not being looked for by each tool. Then the vulnerability or exposure still had to be mapped to the software vendor's name for the problem to get a fix.

Driven by our own attempts to develop an integrated picture of what was happening in our networks and in trying to select some new tools, The MITRE Corporation[6] started to design a method for working through the confusion of vulnerability and exposure information. This method was based on the creation of a reference list of unique names that would then be mapped to the appropriate items in each tool and database. In January 1999 the first public statement of our idea for a

Organization	Name used to refer to vulnerability
AXENT	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
Security Focus	#629 - phf Remote Command Execution Vulnerability

Table 5: *Vulnerability in the Tower of Babel*

reference list of unique names for vulnerabilities and exposures was presented at the 2nd Workshop on Research with Security Vulnerability Databases, held at Purdue University. MITRE presented a paper [1] at this conference that outlined the basic ideas and approach for what is today called the Common Vulnerabilities and Exposures (CVE) initiative.

Our vision for CVE was to provide a mechanism for linking together vulnerability-related databases or concepts – and nothing more (See Figure 1). Rather than viewing this narrow scope as a limitation, we saw it as an advantage. By agreeing to limit the use of CVE to the role of a logical bridge, we could avoid competing with existing and future commercial efforts. This was important, since it was critical that commercial organizations concur with the CVE concept and proceed to incorporate the initiative into their various products and services.

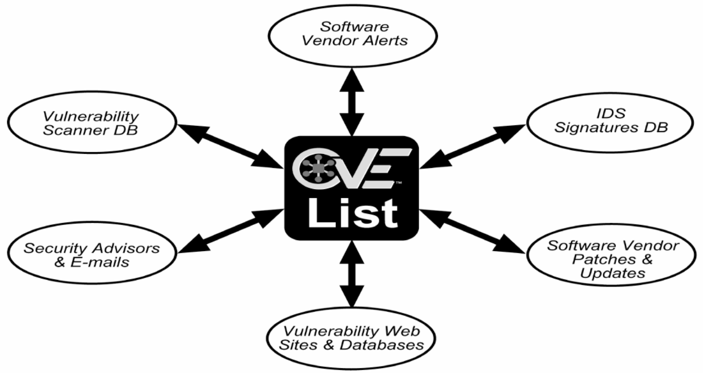

Software Vendor Alerts
Vulnerability Scanner DB
IDS Signatures DB
CVE List
Security Advisors & E-mails
Software Vendor Patches & Updates
Vulnerability Web Sites & Databases

Figure 1: *CVE List as a Bridge*

By March 2001 the CVE effort had evolved into a, cross-industry effort involving more than 30 occupations in creating and maintaining a standard list of vulnerabilities and exposures. Almost half of the known vulnerabilities and exposures are either listed or under review, and presently 29 organizations are building nearly 50 products or services that use CVE names as a key element of their functionality.

How CVE Works

The CVE initiative is an international community activity focused on developing a list that provides common names for publicly known information security vulnerabilities and exposures. The CVE list and information about the CVE effort are available on the CVE Web site at cve.mitre.org/cve/.

The common names in CVE result from open and collaborative discussions of the CVE editorial board. This board, as shown in Table 6, includes members from numerous information security-related organizations around the world, including commercial security tool vendors, members of academia, research institutions, government agencies, and other prominent information security experts. The board identifies which vulnerabilities or exposures will be included in CVE, then determines the common name, description, and references for each entry. The CVE name, for example CVE-1999-0067, is an encoding of the year that the name was assigned and a unique number N for the Nth name assigned that year.

Area of Expertise	Organizations
Academic/Educational	UC Davis, SANS, CERIAS
Network Security Analysts	Vista IT, Genuity
Other Security Experts	IBM Research, MITRE, Zero-Knowledge Systems
Intrusion Detection Experts	Silicon Defense, SANS
Tool Vendors	The Nessus Project, ISS, PGP Security-Network Associates, BindView, AXENT, CyberSafe, Symantec, NFR, Hiverworld, Harris, Cisco
Software Vendors	IBM, Sun Microsystems, Microsoft
Incident Response Teams	CanCERT, CERT/CC, DOD-CERT
Information Providers	NTBugtraq, Security Focus, National Institute of Standards and Technology (NIST), Ernst & Young, eSecurityOnline.com

Table 6: *CVE Editorial Board Composition*

MITRE maintains the CVE list and Web site, moderates editorial board discussions, and provides guidance throughout the process to ensure that CVE remains objective and continues to serve the public interest. Archives of board meetings and discussions are available for review on the CVE web site at cve.mitre.org/board/archives/. Other information security experts are invited to participate on the board on an as-needed basis, based upon recommendations from board members.

The key tenets of the CVE initiative are:

- One name for one vulnerability or exposure.
- One standardized description for each vulnerability or exposure.
- Existence as a dictionary rather than a database.
- Publicly accessible for review or download from the Internet.
- Industry-endorsed via the CVE editorial board and CVE-compatible products.

What Does CVE-Compatible Mean?

CVE-compatible is a phrase that indicates that a tool, Web site, database, or service uses CVE names in a way that allows for a cross-link with other repositories that use CVE names. To be CVE-compatible, the product, service, database, or Web site must meet the following three requirements:

- CVE Searchable: A user can search using a CVE name to find related information.
- CVE Output: Information is presented that includes the related CVE name(s).
- Mapping: The repository owner has provided a mapping relative to a specific version of CVE, and has made a good faith effort to ensure accuracy of that mapping.

Different products and repositories address different portions of the complete CVE list. For example, some might deal with UNIX, while others cover Windows NT. When looking at CVE-compatible items, you will need to evaluate them against your organization's specific needs in terms of platforms coverage and the software products that you use.

Why Use CVE-Compatible Products?

CVE compatibility allows you to use your vulnerability databases and tools together since they can "talk" to each other through shared CVE names. For example, if a report from a vulnerability scanning tool incorporates CVE names, you can quickly and accurately locate fix information in one or more of the separate CVE-compatible databases and Web sites to determine how to fix the problems identified by the vulnerability scanner. Also, with CVE-compatible tools, you will know exactly what each tool covers because the CVE list provides a baseline. Simply determine how many of the CVE entries are applicable for your platforms, operating systems, and commercial software packages, and use this subset to compare against the tool's coverage. Before the use of common names, it was extremely difficult to identify the vulnerabilities of your systems[7], or to determine whether a particular tool or set of tools covered them.

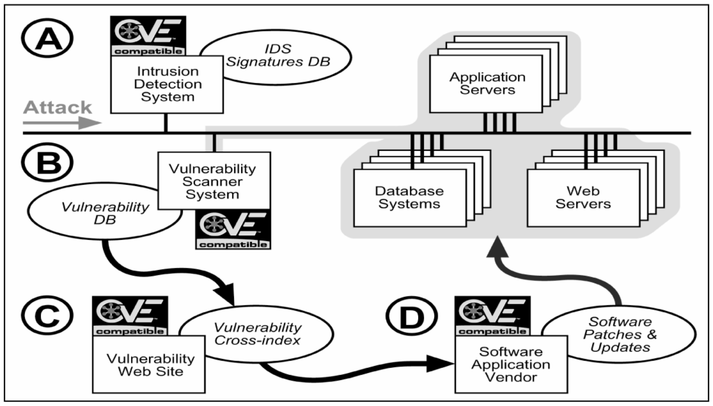
Improving the Process

The CVE effort is changing the way organizations use security tools and data sources to address their operational security posture. The example organization in Figure 2 is able to detect an ongoing attack with its CVE-compatible IDS system (A). In a CVE-compatible IDS, specific vulnerabilities that are susceptible to the detected attack are provided as part of the attack report. This information can then be compared against the latest vulnerability scan by your CVE-compatible scanner (B) to determine whether your enterprise has one of the vulnerabilities or exposures that can be exploited by the attack. If it does, you can turn to a CVE-compatible fix database at the software vendor or you can use the services of a vulnerability Web Site like ICAT Metabase[8], which lets you identify (C) the location of the fix for a CVE entry (D), if one exists.

Identifying Your Risk

Another thing you can accomplish with CVE-compatible products, that would be hard if not impossible to do before common names were adopted, is improve how your organization responds to security advisories. If the advisory is CVE-compatible it will include CVE entries. With that information you can see if your scanners check for these vulnerabilities, and determine whether your IDS has appropriate attack signatures for the alert.

Figure 2: *A CVE-enabled process*



Additionally, for systems that you build or maintain for customers, the CVE compatibility of advisories and announcements will help you directly identify any fixes from commercial software vendors in those systems (if the vendor fix site is CVE compatible). This is a much more structured and predictable process for handling advisories than most organizations currently possess.

Making Guidance Actionable

Earlier this year, a group of concerned security professionals put together a "Top 10" list [2] that outlined the most common, critical Internet security threats. The effort was orchestrated by the System Administration, Networking, and Security (SANS) Institute and brought together a consensus list from a wide variety of security experts. To help bring specificity and make the recommendations actionable, each of the top 10 suggestions had the appropriate CVE names, detailing each of the specific issue areas for a variety of platforms and products. A total of 68 CVE names were called out in the list of 10 threats.

Advanced Research Corporation	Internet Security Systems, Inc.
Alliance Qualité Logiciel	Max Vision Network Security/Whitehats
AXENT Technologies, Inc.	NIST
BindView Development	The Nessus Project
CERIAS/Purdue University	Network Security Systems
CERT Coordination Center	Network Security Wizards
Cisco Systems	NTBugtraq
Computer Security Laboratory, UC Davis	PGP Security, Network Associates
CyberSafe	Qualys
CYRANO	SANS
Ernst & Young	Security Focus, Inc.
Harris Corporation	Security Watch
Hiverworld, Inc.	Symantec
Intranode	Tivoli Systems Inc.
Intrusion.com	World Wide Digital Security

Table 7: *Organizations Developing CVE-Compatible Products*

Who Is CVE-Compatible?

While the list of organizations with CVE-compatible products is expanding, at this writing the vendors in Table 7 are those working toward compatibility. For a current list visit the CVE web site at cve.mitre.org/compatible/.

Today, there are several members of each type of tool, service, repository, and announcement capability that support CVE names. Underrepresented areas are vendor announcement and vendor fix sites; however, several vendors are actively discussing adding CVE names to their announcements. By the time you read this article there should be several vendors using CVE names in their announcements and alerts. In addition, like the CVE editorial board, the list of organizations working on or delivering CVE-compatible products has become international in scope.

Conclusion

The application of all known security fixes and patches is the complement of standard security protection mechanisms. Keeping current on fixes offers a robust method for keeping the commercial software that makes up your organization's software infrastructure healthy. Vulnerabilities and exposures will always be a part of our systems, as will the groups that find and share information about vulnerabilities and exposures in commercial software. With common name integration and cross-referencing abilities emerging in vulnerability and exposure tools, web sites, and databases, it is becoming possible to deal with these mistakes and improve our systems' security. Handling security incidences is more systematic and predictable as CVE is supported within the commercial and academic communities. As vendors respond to user requests for CVE-compatible fix sites, the complete cycle of finding, analyzing, and fixing vulnerabilities will be addressed.◆

On-Line Resources

The on-line resources of this article contain hyperlinks to further references. For the full list please see page 32 of this on-lne version.

References

1. Mann, David E. and Christey, Steven M., Towards a Common Enumeration of Vulnerabilities, 2nd Workshop on Research with Security Vulnerability Databases, Purdue University, West Lafayette, Ind., Jan. 21-22, 1999.
2. Jackson, William, Top 10 System Security Threats Are Familiar Foes, *Government Computer News*, Jun. 12, 2000.
3. Sullivan, Bob, Hospital Confirms Hack Incident, MSNBC, Dec. 9, 2000.
4. Lemos, Robert, Power Play: Electric Company Hacked, ZDNet News, Dec. 15, 2000.
5. Mell, Peter, The ICAT Metabase, Computer Security Division at the National Institute of Standards and Technology, icat.nist.gov/icat.taf Dec. 19, 2000.

Notes

1. Vulnerability is a mistake that someone can directly use to gain access to things they are not supposed to have. An exposure is a mistake that gives that person access to information or capabilities that he or she can then use, as a stepping stone, to gain access.
2. A computer hacker broke into a hospital in the Seattle area and thousands of medical records were downloaded. The hacker's activities went unnoticed by the hospital, and when the hacker went public with his accomplishment, his claims were initially denied. The next day, the hospital confirmed the intrusion [3].
3. A Microsoft Web site was penetrated by a Dutch hacker through the Web server's "IIS Unicode" vulnerability that let him copy files, execute commands, and change files [4].
4. Unlike its original meaning that referred to a hacker as a prolific and inventive software programmer, hacking during the past few years has come to refer to the act of circumventing security mechanisms of information systems or networks. "Black-hat" hackers are those intent on doing harm, as opposed to "white-hat" hackers, who are usually working in support of organizations to help them assess and understand the vulnerabilities and exposures in their systems. Black-hat hackers are sometimes referred to as crackers.
5. As an alternative to tracking and recording each update, patch, and upgrade that gets applied to each platform in the enterprise, the use of vulnerability scanners is an attractive choice for monitoring the health of software applications. These tools are benefiting from the vigor of the market place's hunt for vulnerability information and the development of testing approaches that can turn up the presence of vulnerabilities or exposures in the "deployed" systems of an organization. However, due to "false positives," "false negatives," and incomplete coverage to date, these tools are not a panacea.
6. MITRE, working in partnership with government, is an independent, nonprofit corporation working in the public interest.
7. The CVE initiative is in the process of analyzing and categorizing all of the "legacy" vulnerabilities and exposures, and assigning them CVE numbers. Numerous members of the security vulnerabilities reporting and tracking community have donated their legacy databases to the CVE effort to support this effort.
8. The ICAT Metabase is a searchable index of computer vulnerabilities and exposures. ICAT is not itself a vulnerability and exposure database, but is instead a searchable index leading to vulnerability resources and patch information [5].

Did this article pique your interest?

STC

Would you like to learn more about correcting vulnerabilities and exposures in commercial software that is used to develop your organizations infrastructure? Then attend the Thirteenth Annual Software Technology Conference 2001 on April 29-May 4 in Salt Lake City. Robert A. Martin will speak on this topic in Track 9 on May 2.◆

About the Author

Robert A. Martin is a co-lead for MITRE's Cyber Resource Center Web-site, and a principal engineer in MITRE's Information Technologies Directorate. At the culmination of his five years of Y2K leadership and coordination efforts, Martin served as the operations manager of the Cyber Assurance National Information Center, a 24x7 cyber security watch center within the President's Y2K Information Coordination Center. Today, Martin's efforts are focused on the interplay of cyber security, critical infrastructure protection, and e-Business technologies and services. Martin received a bachelor's degree and a master's degree in electrical engineering from Rensselaer Polytechnic Institute and a master's of business degree from Babson College. He is a member of the ACM, AFCEA, Institute of Electrical and Electronics Engineers (IEEE), and IEEE Computer Society.

Robert A. Martin
The MITRE Corporation, MS B155
202 Burlington Road
Bedford, MA 01730-1420
Voice: 781-271-3001
E-mail: ramartin@mitre.org