

Newsletter of the AICPA
Information Technology Section

What's Inside

FOCUS FOR THIS ISSUE: Information Security and Spam Technologies

1 Application/Network Vulnerabilities and the Risk Management Process

How prone are you to security attacks and what can you do about it? Steve Ursillo Jr. provides an informative perspective, along with an almost-too-real case study.

4 News at 11: Michelle Samuels Channels Fulfilling Career at Broadcast Giant TBS

An InfoTech Update Profile

5 The "Why" Behind CRM Software

Industry expert Anne Stanton offers a practical approach to using CRM to gain momentum, reap benefits and improve the bottom line.

8 Facing Off With the Spam Issue

That darn Spam! With junk e-mail continuing to dominate the headlines, here's a practical how-to article with plenty of referral links from industry tech guru Roman Kepczyk.

9 Emerging Techs: RFID Basics Explain Benefits to Business

In the next few years, RFID will soar to new heights as more and more businesses automate the supply chain process. Discover why RFID made this year's list of emerging technologies.

11 E-Bitz

A cup of Java With "Extra Hot" Security

Are "hot spots" a little too hot for your coffee? Susan Bradley discusses how a seemingly innocent wireless connection can have a tremendous impact on you and your organization.

INFORMATION SECURITY

Application/Network Vulnerabilities and the Risk Management Process

By Steven Ursillo Jr., CPA/CITP, CFE, CISA, MCSE, CIA

Steven J. Ursillo Jr., CPA/CITP, CFE, CISA, MCSE, CIA, is a principal and director of Information Technology and Assurance Services at Sparrow, Johnson & Ursillo, Inc., in Providence, R.I. He specializes in information system security, privacy, control and risk assessments, fraud detection, data extraction and analysis, and technology assurance services. Ursillo chairs the Rhode Island Society of CPAs' Technology Committee, and is a board member and past president of the Rhode Island Chapter of Certified Fraud Examiners.

Advancements in technology solutions continue to provide added efficiency for the most complex and challenging obstacles. However, this forces technology professionals to adapt to rapidly changing environments. Ensuring the confidentiality, integrity and availability of data continues to be a significant concern, from the smallest businesses to the largest public corporations. Every day, emerging security issues and vulnerabilities put some of the most proactive security professionals and network administrators on guard. The nature and technical depth of some of the methods used to exploit systems and security vulnerabilities makes understanding and communicating the risk a continuous challenge.

We know the Internet is still a popular area for attack. At the same time, Internet access and externally hosted services, including a company's Web, mail and FTP servers, force most organizations to have some external presence on the Internet. This external presence increases the risk of, and potential for, different types of external attacks.

The annual CSI/FBI Computer Crime and Security Survey's results of security incidents and attacks over a five-year period (1999 to 2003) indicate that more than half of the respondents incurred an unauthorized use of computer systems within the last 12 months of the years reported. In 2003 alone, 82 percent of respondents had attacks that originated from independent hackers, 77 percent came from disgruntled employees, 79 percent originated from the Internet and 30 percent were from internal systems.

These are some pretty powerful statistics that deeply affect the risk management process. While many mid- to large-size organizations feel these statistics demonstrate a significant threat, there are other businesses and groups that may respond differently. For example, a common response for smaller organizations is to justify a significant reduction of risk because they believe no one is targeting them. Part of that may be true; however, what some organizations may underestimate is that there are many attackers who don't care whom they attack. It is very common for attackers to scan large ranges of IP addresses for

Continued on page 2

InfoTech UPDATE

March/April 2004, Volume 13, No. 2. Publication and editorial office: AICPA, 1211 Avenue of the Americas, New York, N.Y. 10036. Copyright © 2004, American Institute of Certified Public Accountants, Inc. Opinions of authors and the AICPA staff are their own and do not necessarily reflect policies of the Institute or the Information Technology Section. Any hardware or software products mentioned do not in any way represent an endorsement by the Institute or Section.

All rights reserved. You may copy and distribute this document subject to the following conditions:

- (1) Copy all text without modification and include all pages.
- (2) All copies must contain the AICPA copyright notice and any other notices provided therein.
- (3) You may not distribute this document for profit.

Editorial Advisory Board

Susan E. Bradley, CPA/CITP, MCP
Tamiyasu, Smith Horn and Braun
Fresno, Calif.

Mark S. Eckman, CPA
Rockwell Collins, Inc., Cedar Rapids, Iowa

Philip H. Friedlander, CPA/CITP, DBA
St. Petersburg, Fla.

Wayne E. Harding, CPA/CITP
Englewood, Colo.

Roman H. Kepczyk, CPA/CITP
InfoTech Partners North America, Inc.
Phoenix, Ariz.

Janis R. Monroe, CPA
IdentiRISK, Las Vegas, Nev.

Sandi Smith, CPA
Consultant, Dallas, Texas

Anne Stanton
The Norwich Group, Norwich, Vt.

Scott H. Cytron, ABC
Editor, scytron@sbcglobal.net

If you wish to update your member profile, please visit www.aicpa.org/anon/login.asp.

For questions about your subscription to InfoTech Update or other questions about your IT Membership Section benefits, please contact the AICPA at infotech@aicpa.org or leave us a voice mail message at 212-596-6211.

open services and potentially vulnerable system configurations. These attackers are looking to identify externally accessible hosts with particular ports and services that are available for attack.

Are we Really a Target?

Here's a hypothetical, yet disturbingly realistic example. A malicious attacker quietly takes control of an Internet Service Provider's domain name server. The attacker is skilled enough to know that once the system is compromised and full control is available, all evidence of the intrusion will be removed. The attacker implements a backdoor or stealth way of re-entering the system, unannounced to anyone. We will call this system OWNED1. Not only has this system been compromised, but this is just the beginning.

The attacker is now confident that any attack initiated from this system or the next system in line will be difficult to detect, so s(he) quietly accumulates all the functionality need to perform attacks against another host or range of hosts. Next, the process is repeated to gain the unauthorized functionality of another vulnerable system. We will call this system OWNED2. This may be an organization's vulnerable FTP server.

The attacker repeats the concealment process by removing the access trail in the logs, hiding the attacker's working files and setting another stealth backdoor for easy access when needed. This process can be repeated several times in order to make it increasingly difficult for the attacker to be identified. From OWNED2, s(he) sets up an automated port or vulnerability scanner. This scanner is designed to cover a range of IP addresses looking for particular services that have common vulnerability problems, or specifically for newly released exploits that most administrators have not yet managed to patch or update.

In the process of scanning several hundred public IP addresses, the attacker happens to identify ABC Retail Company's Web server. Using a technique to request the

server's banner in conjunction with some other tactics, the attacker can identify the make, version and patch level of the Web server application, and it just so happens s(he) is familiar with a buffer overflow exploit for this version of ABC's Web server application. The exploit was publicized two months ago. The attacker accesses from any number of publicly available sources or develops the appropriate code to take advantage of the application and then uses it against ABC's Web server to gain some privileged access.

From the Eyes of ABC Corporation

ABC Corporation is a \$60 million retail corporation with approximately 200 employees. The corporation's Web site is used for marketing and public relations purposes, and does not incorporate any e-commerce activity. The company management does take security seriously and has participated in several risk assessments with its five-person internal technology staff. ABC runs a state-of-the-art firewall with all the latest security updates. They also have restricted access directly against the firewall.

The system administrators have performed several external scans against their Web server and firewall, and were pleased to report to their manager that the only available access from the Internet was over port 80 — the one needed for people to browse the site. The manager also is aware that the Web server does not contain any confidential information on it. The manager does not seem to believe there is a tremendous amount of risk, short of a Web site defacement or denial of service attack. The feeling is that these types of attacks would be embarrassing, but would not seriously jeopardize the retail sale of their very popular product lines. Besides, the sensitive customer account and credit card information is really on a separate database server without a direct connection.

The latest point-of-sale upgrade consumed the attention of ABC's IT manager, and as a result, he overlooked a security article

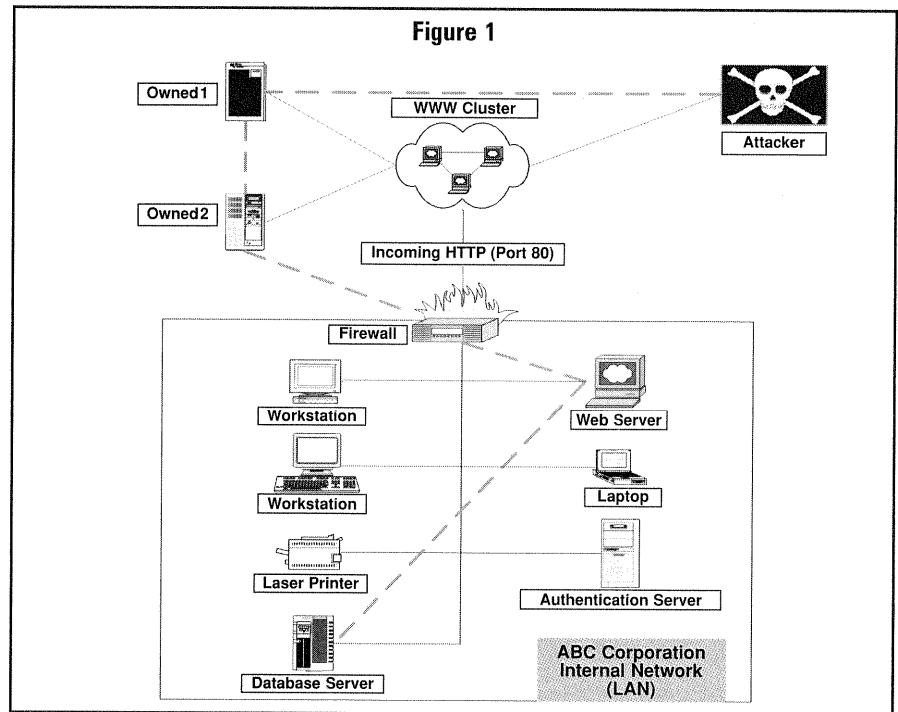
placed in his in-box. The article detailed how buffer overflows are a very common type of system vulnerability that can be targeted to hundreds of types of applications, and that a buffer overflow is the result of a lack of programming bounds checking within the program code.

For example, a particular string (sequence of data) of information within an application is not supposed to contain more than 128 bytes of data. However, if a user enters more than 128 bytes, the excess information forces an override from one area of the computer's memory stack to an alternative location. The result? If the information is entered in a particular way, attackers can inject and execute their own code running at the privilege of the application exploited. If the application is running with system privileges (one step below administrative privileges on Microsoft applications), or, even worse, with administrator or root privileges (powerful access privileges), then the arbitrary code the attacker executes after injecting it from the computer's memory stack will run and function at that same privilege. The overall result would be an attacker gaining full control over the system.

Now Back to the Attacker

The attacker executed a buffer overflow exploit over port 80 — the same port needed for external browsing of the Web site and the only port allowed through the firewall. S(he) has now taken control of ABC's Web server, located on ABC's local area network (LAN) as diagrammed in Figure 1.

ABC's management already addressed the risk of the Web server being compromised. The attacker can deface the site or even shut down the Web server. That was considered somewhat tolerable, right? Unfortunately, it can get much worse! The attacker has fully compromised and controlled the Web server, and this server is on the corporation's LAN. Once this occurs, the attacker can perform "island hopping" or attack one host at a time, similar to what was performed with OWNED1 and OWNED2 in order to hide the trail.



The attacker can now capture network data and traffic with a network sniffer, capture user credentials, capture and map out host information, and view critical configuration settings. S(he) now has a clear line of attack against any host located on ABC's LAN, and the hosts on the LAN do not have any firewall protection between them. After attacking and compromising the database server, the attacker parts with ABC's customer database; including credit card information; hides the entry trails on all systems compromised by deleting access and activity logs, and also hides used files. A back door is set for periodic follow up and undetected remote access back to ABC Company's LAN. This attacker may not have ever heard of ABC Corporation, but only followed the exploit. Let's just hope the attacker does not decide to post the back door access credentials on some underground hacking Web site, chat server or newsgroup for all other hackers to use as well!

An Ounce of Prevention

There are a few actions and controls that could have prevented this attack from occurring. Most buffer overflow exploits

that are released force vendors to respond with an update or patch for the program or application flaw. In many ways, this can become a race to keep up. System administrators should follow best practice skills for implementing any patch or program update, which usually requires that the application and system be tested before going live into production.

Sometimes a lack of time or resources allows this process to occur improperly, which initiates added availability issues and risk. However, if an exploit is publicized, attackers may be aggressively trying to identify those companies who have not yet had the time to respond. If the attacker beats the administrator to the punch and sets a stealth backdoor after compromise, the damage is already done. Even though the system was updated and the vulnerability is no longer present, the back door, most likely, is still available. In the ABC Company example, the administrators are balancing the risk of a known system vulnerability and the risk of applying any untested patches that may affect the performance of their production system. Ideally, timely testing and implementation of the updates is the best

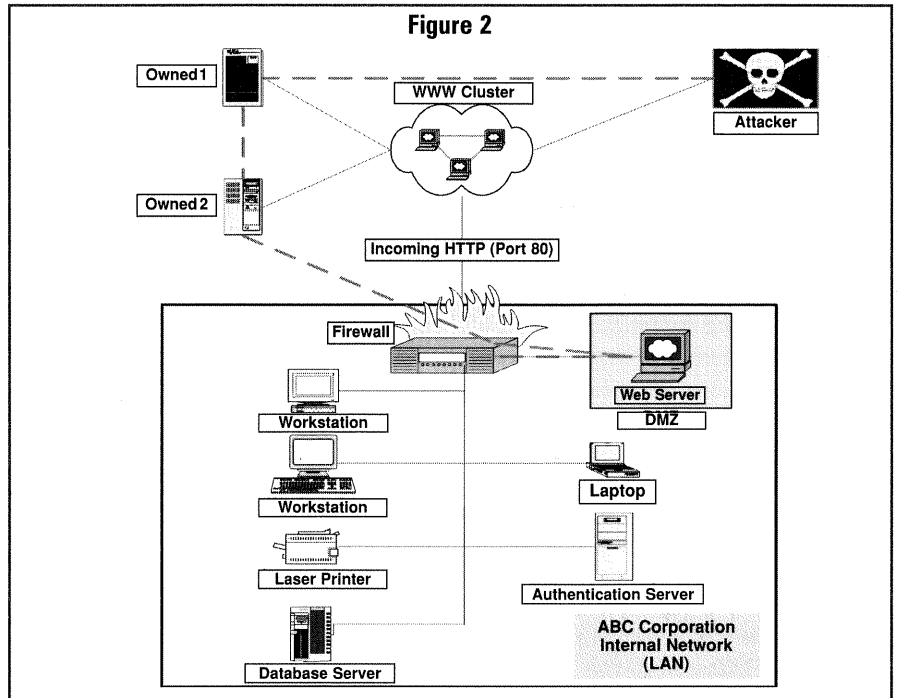
Continued on page 4

solution, but this decision comes from the managers and those who have an intimate knowledge of ABC's systems and infrastructure.

ABC's network architecture is another area the company could have modified in order to manage the risk of compromise. Had ABC's Web server been placed on an isolated network segment, otherwise known as a demilitarized zone (DMZ), the risk would have been reduced by containing the single vulnerability to the Web server. The same attack with a change in the network architecture is diagrammed on right in Figure 2.

In this figure, we see that once the attacker gains control of the Web server and the rest of the internal LAN is still protected by the firewall. The attacker would have to initiate an attack back through the firewall from the Web server to try to get to the LAN.

A buffer overflow — one of the most common types of Internet-based attacks — is just one of many types of system vulnerabilities that can come about over time or as new application flaws are discovered. Even though statistics show that an organization's most significant risks comes from insider abuse, it is clear that external threats are something that should not be underestimated. Proper risk assessment, proactive security monitoring, assessments



and assurance services should be used in order for management to obtain a comfort level that follows the organization's security policies and culture.

.....
For more information on risks associated with security vulnerability, plan to attend Steven Ursillo Jr.'s session on this

topic at Tech 2004, May 3-5 at the Venetian Resort & Casino in Las Vegas. Visit www.cpatechconf.com for registration and an online brochure.

Contact Steven Ursillo Jr. at sursillojr@sju.com. ●

INFOTECH UPDATE PROFILE

News at 11: Michelle Samuels Channels Fulfilling Career at Broadcast Giant TBS

By Tim Elsner

As a self-described "business and industry gal," Michelle Samuels, CPA/CITP, CQM, prefers the type of accounting work she calls "in the action" — or in the details, creating a company's financial statements while serving as an integral part of its decision making process.



Michelle Samuels

Ten-plus years after joining Atlanta-based Turner Broadcasting System, Inc. (TBS), one might say that as director of Financial

Compliance, Samuels is certainly *in* the action — and more. After all, this is the 8,000-employee, multifaceted company whose cornerstone property revolutionized broadcast news coverage with its groundbreaking 24-hour news channel, CNN. And that's just one network (albeit a key one) in the news division. Today, TBS includes, among other businesses, numerous entertainment networks (TBS, TNT, Cartoon Network), the Atlanta Braves, many Internet sites (cnn.com, nascar.com, pga.com), other professional sports interests and even real estate.

These holdings add up to Samuels' appreciation and exposure to a variety of businesses within a business, as well as many aspects of information technology (IT) and accounting.

Continued on page 5