# Mitigating Security Issues:

## The University of Memphis Case

*A compromised server at the University of Memphis highlighted the security risks faced by complicated systems on campus*

By **Robert Jackson** and **Mark N. Frolick**

Organizations invest substantial resources developing complicated solutions that are critical to daily operations and long-term success. With the recent economic downturn and shrinking budgets, IT departments are seeking even more efficient ways to solve problems. Many organizations have turned to external vendors for assistance because of their ability to provide products that seamlessly integrate with other critical infrastructure pieces in an organization, as well as their software's ease of use. This trend has resulted in a new era of empowerment for users who otherwise might not have the technical knowledge to solve many IT problems.

Empowerment of users and experimentation in the learning process, however, often cause organizations to struggle with security issues. Some organizations discover that empowering nontechnical users results in the security exposure of networks, applications, workstations, or servers. These exposures threaten the stability of the IT environment and, if left unattended, can result in compromised servers and possibly lost data. Security policies should exist to prevent unauthorized access, malicious acts, or accidental destruction of data.

This article presents a case study of a security vulnerability faced by the IT department at the University of Memphis. Relevant issues involving teamwork and cooperation between server and service administrators are considered, along with recommendations on how organizations can mitigate security vulnerabilities in their own installations.

### The University of Memphis Server Security Breach

This study of a compromised server at the University of Memphis reviews various personnel roles, detection of the compromised server, policy enforcement, forensics, and the proactive search for other servers facing the same security exposure.

#### *The Stakeholders*

The University of Memphis IT department includes several groups responsible for various functions. For the purposes of this particular study, the Intel Server Support Team (ISST) consists of server administrators who are responsible for the security and well-being of the Windows-Intel servers. Service administrators, including Web designers and database analysts, are responsible for applications that run on various server platforms. The compromised server was running the Microsoft Windows NT4 operating system with service pack 6,

MS-SQL 6.5, and IIS 4 in addition to an older version of PHP. MS-SQL is Microsoft's flagship relational database product, Internet Information Services (IIS) is the company's Web server product, and PHP is a programming tool used by Web developers to quickly develop dynamic Web pages.

### Detection of the Compromised Server

In 2002, ISST received a warning message from the server-monitoring software, Big Brother, regarding disk space on the affected server. Upon inspection, ISST discovered large amounts of disk space were being consumed by file structures hidden within the Windows recycle bin. This hidden file structure was sufficient proof that the server had been compromised. The issue then became how to take an important server off the network.

### Enforcing Policy

ISST immediately notified a director who was routinely involved with the university's security infrastructure. After evidence of the compromise was presented, ISST and the director agreed the server had to be disconnected from the network. Proper officials within the department were notified of the server's compromise, and they reluctantly agreed that it should be disconnected from the network. The server was disconnected from the network, and recovery efforts were started.

The decision to remove this server from the network was particularly difficult because of its profile within the university environment. It was the university's online knowledge base and had been growing in popularity following a series of promotions by the department.

Restoring this service required 12 hours, for several reasons: debates that ensued over whether the compromised server could be returned to service, attempts to recover data from the server instead of from backup, time required to rebuild the server, and time required to reinstall all necessary applications. Clear security policies and procedures could have eliminated confusion that occurred during this phase by clearly spelling out to various staff members actions to be taken in the event of security compromises. This is a good time to remind the reader how important it is to have the full support of management when implementing and enforcing a security policy.

### Forensics

A forensics investigation revealed that hackers gained access to the system through a blank password on the "sa" account of MS-SQL. Although the service administrators stated a password did exist for that account, the ISST group determined that log entries indicated the "sa" account had been used to compromise the server. It is likely that the default installation of MS-SQL resulted in a blank password being assigned to the "sa" account. Upon connecting to the server with the open "sa" account, the hackers used the xp_cmdshell procedure, the result of a default installation, to execute appropriate commands to gain full access to the server. Once full access was obtained, the hackers installed an FTP server on the machine and began to utilize the university's bandwidth and storage capacity for illegal means.

It is important to note the disparate facts presented by ISST and the service

administrators. Teamwork and cooperation were called into question when ISST presented the results of the forensic investigation. The goal of any forensic investigation should be to inform and educate, not to place blame.

### *Search for Other Vulnerable MS-SQL Servers*

Realizing there were probably other servers on campus running MS-SQL, ISST was directed to perform scans of other servers to determine the university's vulnerability. Although four additional servers were located with no "sa" account passwords, this turned into a political issue for the ISST group when their actions and methodologies for disseminating information were questioned. This is another example of how a security policy could be used to improve communication among various groups within the department. Setting clear guidelines within the security policy would tell all parties what to expect in the event of security exposure.

### *Summary*

The server was compromised because the MS-SQL "sa" account did not have a password assigned. The server was wiped clean, rebuilt, and placed into service after 12 hours of downtime. The political fallout from the compromised server resulted in a meeting with the server administrators, service administrators, and IT management to discuss security policies and procedures. The meeting highlighted the challenges faced when the concepts of teamwork and cooperation confront the stress caused by a server compromise.

### *Lessons Learned*

First, it is very important that management include security as part of the mission and vision for the IT department. Without appropriate security policies and procedures, it will be difficult to ensure stable computing environments. These security policies will also serve as an educational tool, clearly indicating actions to be taken when compromised servers are detected.

Second, equilibrium between experimentation and security standards must be established. It might not be appropriate to deploy an application into a production environment unless appropriate security testing has been performed. The IT department at the University of Memphis is currently attempting to address this issue through a change control process that includes thorough testing in development and preproduction environments before moving into production.

**Setting clear guidelines within the security policy would tell all parties what to expect in the event of security exposure.**

Finally, teamwork and cooperation must be stressed during times of security exposure, especially when a compromised server is discovered. Server administrators must work with service administrators to return a service to production as quickly as possible. At the same time, service administrators must understand the importance of securing, and keeping secure, the production environments that services depend upon.

Communication between groups is one of the most important obstacles to overcome when striving to obtain secure environments and when dealing with security breaches. As previously mentioned, teamwork and cooperation also play a role in making sure the organization works together. However, there are some issues that server administrators can address unilaterally. To that end, we can make several recommendations to mitigate security exposure.

## Recommendations to Mitigate Security Exposure

With the constant threat of attacks and the improvements hackers build into viruses and hacking tools, the question is not "if" a server will be compromised but "when." Organizations can mitigate some of the possible security exposures by exercising a few precautions: be observant about network and server activity, seek knowledge about current security risks, be proactive in patching and securing servers, diversify technology platforms if possible, require complex passwords, keep an open mind about the ongoing struggle, and be prepared when the compromise occurs.

### *Be Observant*

Tools should be acquired that will assist in monitoring the network. Intrusion detection system (IDS) software such as SNORT assists in monitoring network traffic. Anti-virus software such as Norton AntiVirus provides a line of virus defense in the event systems are vulnerable to attack. Programs like Big Brother monitor various aspects of a system and can be configured to page or send e-mail notifying appropriate staff of any alarms. Other programs provided by companies like Bindview can be used to monitor and protect servers. Log analysis products such as InTrust assist in evaluation of logs to identify any patterns of strange activity.

Many tools do an excellent job of reporting. Given the limited time many support personnel can devote to security, such tools might seem a boon for automating day-to-day tasks. Even when supported by such tools, however, IT staff would be well advised to manually review logs, disk drives, processes, and other server properties at fairly regular intervals. After all, some recent viruses (such as Bugbear) have disabled anti-virus programs and other protective measures.

### *Seek Knowledge*

The battle against hackers and viruses is never won. By seeking knowledge to keep up with the field, IT staff can take preventive action before a hacker or virus damages the organization's network. Management and support personnel can benefit from various e-mail lists and Web sites that exist to educate people about security issues.

The following Web sites are excellent sources of information:

- <http://www.sans.org>
- <http://www.cert.org>
- <http://cve.mitre.org>
- <http://isc.incidents.org>

SANS is a leader in the security field. Their Web site contains links to educational opportunities as well as current security issues.

The CERT Web site contains information on a variety of Internet security problems.

CVE maintains a list of "Common Vulnerabilities and Exposures." Nessus, an internal network scanning product, relies on the CVE database to identify potential vulnerabilities during scans.

Isc.incidents.org is a very good Web site to consult for current worm and other incident activity on the Internet. This might be particularly useful for outbreaks of worms like the so-called "MS-SQL Slammer."

At these Web sites you can obtain information about specific vulnerabilities, recent virus attacks, tools to assist with security, training opportunities, and more. For those people supporting Microsoft platforms, a helpful Web site is <http://www.microsoft.com/technet/security>.

### *Be Proactive*

Apply patches regularly. In an enterprise environment where administrators have many servers to maintain, a product such as Update Expert by St. Bernard Software will save a great deal of time. This program can be configured to automatically download and install selected patches during off hours. Scan the internal network with a product such as Nessus (found at <http://www.nessus.org>). By scanning the internal network, the server administrator can take a proactive stance on addressing security vulnerabilities.

### *Diversify*

Using varied technologies for operating systems or critical infrastructure can insulate systems from attack. For example, viruses, worms, or hacker tools written for a specific operating system might not be effective on other platforms.

### *Use Complex Passwords*

Commonly, viruses attack servers by exploiting a default user name for the "administrator" account or password. Changing the administrator account name to something more complicated such as "@dmin" or something less likely to be guessed by a virus writer can easily defeat this type of script. Complex passwords containing characters like @#$!*& should be used for all accounts. Use a product like L0phtcrack 4 (from <http://www.atstake.com>) to determine if your organization is using complex passwords.

### *Keep an Open Mind*

Identifying all the security issues faced by organizations is a daunting, if not impossible, task. It is important, however, to keep an open mind and discuss these issues openly. Microsoft, for example, announced the "Trustworthy Computing" initiative and released several patches this year while delaying the release of new products. Security issues are not isolated to the Microsoft platform, of course. The company is often singled out because it is a large target and its software has weaknesses. Vulnerabilities are constantly discovered for UNIX operating systems as well.

### *Be Prepared*

Ensure that enforceable policies and procedures exist. Make sure those policies and procedures are understood and supported by management. Perform regular backups and test the backups to ensure that data can be recovered from the backup media. The restore test should include someone examining the restored data to ensure that it is valid and readable. Also, determine if there are phasing issues with backups, such as running the backup process too early to catch important data typically written to the system later.

Find ways to reduce recovery time, for example, by using products such as PowerQuest's PowerDeploy or Symantec's Ghost. Keep in mind, however, that restoring an exact duplicate of a system might also restore the vulnerability that was exploited by an attacker.

An excellent program to have for the Windows platform is ERD Commander (from <http://www.winternals.com>). This program contains utilities that allow access to non-bootable versions of Microsoft operating systems, potentially enabling recovery of the server.

Carefully review products before deploying them onto a server. Reviewing the software gives IT staff an understanding of whether, in addition to meeting functional requirements, it is secure. Security issues must be considered during application development and deployment, not after software has been placed into a production environment.

## Conclusion

Organizations must accept that security exposure is commonplace. Management must accept that with some technologies the price for ease of use, integration, and functionality is often poor security. Management should work with support staff to ensure that adequate procedures and policies are in place to protect the organization under these circumstances. In addition, management should accommodate the applications development group by providing more time during project planning to be devoted to researching security issues.

To adequately secure the computing environment requires communication, cooperation, and teamwork among many different personnel throughout the organization. In addition, procedures and policies must exist to address security compromises when they occur. Server and service administrators must have a clear understanding of their roles and how they can work together to build a secure environment.

Organizations should strive to harden their environment by ensuring that the latest patches are installed, virus protection is in place, and proper monitoring of the network is occurring. In this regard, it is important to take a proactive stance in developing and communicating an appropriate security policy as organizations continue to struggle with security issues. *e*

---

*Robert Jackson (rjax@memphis.edu) is a Systems Administrator in the Information Technology Division at the University of Memphis, Tennessee. Mark N. Frolick (mark@frolick.net) is the Western and Southern Financial Chair in Information Systems at Xavier University in Cincinnati, Ohio.*