Realtime publishers

"Leading the Conversation"

The Essentials Series

IT Compliance Volume II

sponsored by

SECURE COMPUTING

by Rebecca Herold

Addressing Web-Based Access and Authentication Challenges

by Rebecca Herold, CISSP, CISM, CISA, FLMI *February 2007*

Incidents Occur When Controls Are Weak

Many incidents occur through access and authentication vulnerabilities. Let's look at some highlights of a recent event that may have been the result of such weaknesses.

- Sometime in December 2006, TJX Companies Inc. discovered vulnerabilities in their computer systems and networks that allowed unauthorized access to their data, including their customers' personally identifiable information (PII).
- On January 17, 2007, TJX announced its computer network that handles customer transactions for around 2500 retail stores was hacked into, and PII, including credit, debit, and driver's license information, was stolen.
- On January 22, the Massachusetts Bankers Association (MBA) said that banks had to cancel and reissue cards affected by the breach and that the banks that issued the cards, rather than individual consumers, would cover all fraudulent purchases.
- On January 24, the MBA said that fraudulent use of the stolen debit and credit card information from the TJX breach had been reported by banks in Florida, Georgia, and Louisiana, as well as overseas.
- On January 29, AmeriFirst Bank in Alabama bank filed a federal class action lawsuit in Massachusetts against TJX in an attempt to recover the costs of a breach incident the bank alleged was the result of negligent data security practices by TJX.
- On January 29, a complaint seeking class action status was filed in federal court in Massachusetts on behalf of all TJX customers in the United States against TJX for negligently failing to adequately secure its customer information. The single count common law negligence complaint alleges TJX did not comply with the Payment Card Industry Data Security Standard (PCI DSS).

As you can see, this breach impacted many entities: TJX, their business partner banks and retailers, credit card companies, and customers. And the fallout continues. Not complying with the PCI standards can also result in fines on merchant banks and retailers. And there are many other federal and state-level laws and regulations that may also be applied, such as the Gramm-Leach-Bliley Act (GLBA) and the FTC Act, to name just a couple.

VISA imposed $4.6 million in fines in 2006 for PCI noncompliance, up from $3.4 million in 2005.

There have been many other incidents that resulted from exploiting weak authentication and access controls. Organizations must ensure applications and systems are built using strong information security practices. If they aren't, the impact could not only be huge, it could linger on for many years, or even close the business.

This paper focuses on two important aspects of applications and systems security—authentication and access controls. Business leaders must ensure they are implemented effectively to help protect the business as well as PII.

Web Authentication Issues

Significant security vulnerabilities can exist if Web applications do not implement authentication mechanisms appropriately. The issues differ for authentication for those who only occasionally use the application, those who regularly use the application, and those who must provide support to the application.

Historically, single-factor authentication, in the form of an identifier and password, was used for Web authentication. However, there are several realities that make single-factor authentication quite vulnerable to defeat:

- Passwords can be inappropriately shared with others. Check the monitors for sticky notes within most organizations and you will likely find several passwords; not to mention the executive assistant to the VPs who has a nicely documented list of all their passwords and identifiers by his keyboard.
- Most people create poor passwords that can be easily guessed, whether by chance or through the use of any number of freely available password crackers.
- Clear-text passwords in transit are vulnerable. There are a large number of clever communications eavesdropping tools available to collect passwords as they pass through network transmissions.
- Encrypting passwords in transit doesn't provide comprehensive protection. Keystroke loggers are increasingly used to record passwords and then send them to criminals to use to gain access.
- Clear-text passwords in storage are vulnerable. If there are weaknesses in the system housing the passwords, hackers may be able to get to the password file.
- Single-factor authentication implementations can be vulnerable to man-in-the-middle and Denial of Service (DoS) attacks.

The U.S. government saw these risks and reacted to protect consumer PII by recently requiring banks to implement multi-factor authentication on their Web sites. The Federal Financial Institutions Examination Council (FFIEC) considers single-factor authentication as inadequate for transactions involving PII, and on October 12, 2005, issued updated guidance requiring financial institutions engaging in any form of Internet banking to use effective methods to authenticate the identity of customers using those products and services. Based upon the result of risk assessments, financial institutions must implement multi-factor authentication, layered security, or other controls reasonably configured and implemented to mitigate those risks.

> 🕮 The FFIEC Interagency Guidance on Authentication in an Internet Banking Environment can be found at http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/ots-ceo-ltr-228.pdf.

Multi-Factor Authentication

To implement multi-factor authentication, at least two of the following three items are used with the identifier to authenticate:

- Something you have, such as a security token, credit card, proximity badge, and so on
- Something you know, such as a password, PIN, passphrase, and so on
- Something you are; a biometric attribute, such as your fingerprint, voice pattern, retinal scans, and so on

There are challenges in implementing a multi-factor authentication solution for Web applications. Just a few include:

- Deploying the "something you have," such as security tokens, to all users. This may be a significant undertaking for an organization that wants to deploy to all their customers.
- Successfully and effectively communicating to a diverse group of users how to be able successfully use the security tokens they receive.
- Deploying the "something you are" factor may not be feasible for some organizations to use with their customers, depending upon the numbers involved and how much support they can make available to the customers.
- Using multi-factor authentication could cost a significant amount of money to deploy.

Most organizations deploying multi-factor authentication determine that using passwords or PINs in combination with a security token is the best solution to meet multi-factor authentication requirements.

Access Control Issues

Once an individual is authenticated, you must be sure to limit the individual's access to only those systems and applications resources for which the user is approved. User accounts must be given the least privileges necessary not only to provide strong security to protect systems and information resources but also to meet the growing numbers of laws and regulations that require least privilege access. Just a couple of U.S. laws that have this least privilege requirement include GLBA and the Health Insurance Portability and Accountability Act (HIPAA), in addition to the FFIEC guidance discussed earlier.

Organizations must address multiple issues for Web-based application access controls. A comprehensive security policy utilizing a system that centralizes management can be implemented to be successful with access control efforts. A comprehensive and effective Web access solution should have the capabilities for:

- Endpoint security and configuration compliance enforcement and reporting capabilities—Inappropriately configured servers, as well as remote devices, create threats to the organization's systems and information resources; malware could enter the organization, unpatched systems could be exploited and have a chain reaction impact to the internal systems, and so on. There should also be ways to ensure each system has the latest software releases and complies with corporate firewall and security policies.
- Centralized access management to protect intranet and extranet resources—You should be able to establish least privilege and role-based access through one utility to be most efficient, not leave security holes, and ensure appropriate access settings and security.
- Centralized policy reporting—Organizations often have to run multiple reports for each of the many access points to their network. An effective solution will be able to pull all audit logs and reports together for more efficient reporting and review as well as to create the documentation necessary to comply with multiple laws, regulations, and contractual requirements.
- Centralized policy enforcement—Ensuring all applications and servers have been appropriately updated to meet new policies and address new threats can take a significant amount of time. An effective solution will be able to ensure the policy updates are distributed to all servers and systems, significantly easing the policy update activities.
- Anywhere, anytime remote access to applications, data, and networks. With customers, personnel, and business partners scattered all over the world, limiting the time applications are available is no longer an option for most businesses.

Some of the basics for Web application authentication and access control security include:

- Limiting the services offered by the computer running the Web server to a minimum
- Limiting the number of users with most privileged access, such as Administrator in NT or root in UNIX, to a minimum
- Limiting the number of accounts on each system to the minimum needed
- Performing regular risk analysis and vulnerability assessments
- Changing the default settings on systems to more secure settings
- Applying security patches on a timely and ongoing basis
- Logging key events—such as failed and successful logins, attempts to access files/directories without authority, successful and failed attempts to access sensitive data—to help ensure accountability and for troubleshooting purposes

Logs often contain sensitive information such as dates and times of user access. Logs containing sensitive information should be accessible only to authorized staff and should not be publicly accessible.

- Removing all sample scripts from Web servers and Web development tools; they often contain well-known security holes that potential intruders try to exploit
- Checking regularly to ensure sensitive data files were not created within temporary directories by Web development tools as a side effect
- Encrypting sensitive data collected through the Web application, accessed by the Web application, or stored on the Web server

Some versions of SSH1 are vulnerable to a buffer overflow in the authentication phase of establishing a SSH tunnel. Snort rule 1327 will identify this ssh-crc32exploit.

It Can Be Done

Although there are challenges, Web application authentication and access controls can, and must, be deployed securely. Organizations have succeeded. Regional MLS (RMLS), a real estate multiple listing service (MLS) in Florida, is a case in point. IDC did a case study of RMLS' Web authorization and access security implementation.

> 🕮 View the IDC RMLS case study at http://www.securecomputing.com/pdf/SS_RegionalMLS-IDC.pdf.

Real estate professionals possess a great amount of PII, along with sensitive information about real estate details, which must be kept from public access. Controlling access to the MLS, transaction management systems, and broker systems, has become increasingly critical because it is no longer simply the listing information that is at risk. Concern for privacy and preventing data breaches must be a priority for real estate professionals.

MLS systems typically include contact management and CRM applications that store PII about clients and prospects. RMLS is subject to federal regulations such as the Sarbanes-Oxley Act (SOX) and GLBA that require safeguards to protect this confidential customer data.

RMLS had observed that their MLS subscribers, including the agents, secretaries, and assistants, were often sharing their systems identifiers and passwords with many other third parties. RMLS realized that these activities put the PII within their systems at great risk, and put them in noncompliance with applicable laws and regulations. They determined that the most effective way to address this was to use a centrally managed access control system in conjunction with an authentication method that would involve passwords that could not be shared.

To address the regulatory requirements and the vulnerable security practices, RMLS did some research and began deployment of more than 17,000 security tokens for multi-factor authentication to their MLS subscribers in the summer of 2005 as part of their implementation of Clareity's SAFEMLS security access control system paired with Secure Computing's SafeWord PremierAccess authentication technology.

> 🕮 Find information about the Clareity Security SAFEMLS system at http://www.safemls.com/. Find information about the Secure Computing SafeWord PremierAccess authentication technology at http://www.securecomputing.com/index.cfm?skey=643.

RMLS reported the deployment was successful and that the subscribers were happy with the solution. No cost was passed on to the subscribers for the tokens, unless they lost one and had to replace it. During implementation, all users were required to pick up their tokens from the RMLS facility. Before they were issued tokens, they had to attend a 30-minute security training session. Since the initial roll-out, RMLS sends new users security information and gives them the option of either picking up their token at their facilities or receiving it by mail.

Pairing Multi-Factor Authentication with Access Control Is Effective

Multi-factor authentication removes most of the risks involved with just using a password. Using security tokens as the multi-factor authentication solution of choice provides protection against:

- Transmission eavesdropping
- Keystroke loggers and replay
- Online guessing
- Impersonation and spoofing
- Man-in-the-middle attacks
- Session high-jacking

Implementations using security tokens that integrate with centralized access controls work well to help prevent many kinds of security compromises while addressing regulatory and contractual requirements to protect sensitive information. With thoughtful planning, implementation can be efficient and effective, even with end users who are geographically dispersed.