

Information Security in the Internet Age
Securing World Wide Web Applications

Information Security in the Internet Age

Securing World Wide Web Applications

Overview

Information security vulnerabilities have increased dramatically with the proliferation of corporate web sites, Internet-based customer relationship management software, online business-to-business collaboration, and electronic commerce. Criminals are getting increasingly sophisticated with their techniques and targeting their attacks on the software that is driving the Internet age.

Introduction

Internet software attacks have become a key threat to corporate and information security. The types and frequency of these cyber-security attacks have increased considerably in the past several years. The media is hungry to report successful attacks on corporations and how their customers may be affected. The following recent articles describe results of using non-secure Internet applications.

“By 2009 80 percent of companies will have suffered an internet application security incident”

- Gartner Research Group

. . . the vulnerability assessments conducted concluded that at least 92 percent of web applications are vulnerable to some form of hacker attacks. While these types of hacking attacks are common, most enterprises have not adequately secured web sites, applications and servers against them.

More robust network security has driven hackers to view web applications as easier targets.

Both State and Federal legislation has been passed which is designed to protect consumers by imposing regulations on companies and organizations, and charging penalties on those that fail to comply. These regulatory obligations require that companies take appropriate measures to secure information.

Health Insurance Portability and Accountability Act of 1996

One of the main goals of the Health Insurance Portability and Accountability Act (HIPAA) is to protect the security and confidentiality of electronic health information. HIPAA required the United States Department of Health and Human Services (DHHS) to develop security requirements for health information that identifies individual patients. *All healthcare organizations that maintain or transmit electronic health information must comply or risk significant financial penalties.*

Gramm Leach Bliley Act of 1999

The Gramm Leach Bliley Act (GLBA) required financial institutions to have a comprehensive written information security program in place by July 1, 2001. The GLBA applies to all banks and federal branches of foreign banks that are subject to the supervision of various regulatory agencies including the Federal Reserve, OTS, OCC and FDIC.

The purpose of GLBA is to give these regulatory agencies a charter to oversee the protection of the security and confidentiality of non-public customer information. Each financial institution is required to implement a comprehensive written information security program. The information security program must be designed to:

- ✓ Ensure security and confidentiality of customer records and information
- ✓ Protect against any anticipated threats or hazards to the security or integrity of such records
- ✓ Protect against unauthorized access or use of records or information that could harm or inconvenience any customer

Each financial institution is responsible for assessing, managing and controlling the risk to their customers' information. Given the inherent risks of the Internet, companies that use the Internet for commercial transactions have a much higher potential risk to customer information than those that do not. The four requirements of an information security program under GLBA are as follows:

- ✓ Identify and assess risk

- ✓ Document policies and procedures for controlling risk
- ✓ Update the program to keep pace with technology and threats
- ✓ Implement and test the plan

Trends

To compete in today's economy, companies and organizations are putting more information and services on the Internet. When customers help themselves, everyone wins. But the risks are great. Criminals who use the Internet for their nefarious acts have their own communities, with online collaboration, downloadable tools, and live conventions. The media has picked up on the newsworthiness of successful security breaches, and company stock prices can be severely impacted from such attention.

The prime targets for cyber-attacks are government, financial services, media/entertainment, and power and energy companies; however any company that stores non-public personal information may potentially come under attack. Cyber-terrorism has also become a real threat to the infrastructure that is increasingly dependent on the Internet. Even more disturbing is that many sophisticated cyber-attacks are attributable to organized crime, whose resources are far greater than the traditional 'hacker'.

Criminals are using automation to increase the speed and efficiency of their attacks. Attack tools use advanced scanning techniques to maximize their impact. They can self-initiate new attack cycles. Recent computer viruses self-propagated to global saturation in less than 18 hours.

Criminals are using advanced engineering techniques that make it difficult for security experts to detect the tools and easy for hackers to evolve them. The number of reported software vulnerabilities discovered is doubling every year, and hackers are exploiting them faster than vendors can patch them. New technologies are being introduced by vendors that bypass typical firewalls - for example, WebDAV (Web-based Distributed Authoring and Versioning).

Most companies focus security efforts on hardening the perimeter of the network and the operating systems of machines on that network. However, there is more to security than deploying the latest firewall hardware and intrusion detection systems. Many attacks consist of **Internet-based information requests** that are **indistinguishable from normal customer use**. The easiest method to attack a company may just be straight through a customer service web-facing application. All too often in software development, computer programmers focus on delivering functionality and leave security as an afterthought, which frequently results in exploitable vulnerabilities in the application, such as cross-site scripting, buffer overflows, etc.

AsTech Strategy

To develop a good prevention strategy, one must first understand how a hacker works. Before an attack can be launched, a hacker will gather information about the target environment by using scanning tools. **Knowledge** about how these tools work and how applications are *foot-printed*, allows us to recommend methods of concealing details about the application production environment.

Poor error handling, use of sensitive data on the client-side of the application, and careless deployment architectures are a few of the problems that may be present in applications that give hackers launching points for their attacks. Authentication and access control are commonly exploited and must be carefully coded or integrated using standards that have been developed and tested in real world environments.

Criminals may also use published information about software security bugs and anything else they may find out about the software from message boards, employees, etc. All that is needed is to find one critical weakness to exploit. Knowing how hackers have exploited applications in the past, gives us **insight** into how an application may be attacked.

A common security problem in many web applications today is the lack of input validation. By inserting special scripting characters into a web-facing application data field, it may be possible for an attacker to execute malicious code on customers' web browsers. With this exploit, an attacker may also be able to deceive an application administrator into sending his or her login name and password to the attacker. In fact, under the right circumstances, this exploit is powerful enough to expose or corrupt the entire contents

of the application's database. These kinds of attacks can also be successful even against carefully developed applications, using a variety of clever techniques.

AsTech Consulting has developed a comprehensive set of security coding standards designed to serve as a **benchmark** for application security. With knowledge of past exploits, our coding standards are designed to protect applications from the vast majority of hackers and their tools. Our security coding standards cover common issues, like access control and session management, as well as language-related issues, such as C buffer overflow exploits. Much like virus detection software, our coding standards are constantly updated as technology evolves and security notices are published.

By using experienced programmers trained in advanced security techniques, AsTech Consulting aims to protect applications from the most intelligent attack forms. Our security code review team has **experience** securing applications for the health and financial industries, under the most stringent regulatory guidelines. Our review group is knowledgeable in a variety of platforms, architectures, deployment frameworks, and programming languages, including but not limited to: UNIX, Windows, J2EE, Windows DNA, .NET, WebLogic, WebSphere, Dynamo, Java, ASP, C/C++, PERL. Our detailed understanding of cryptography and encryption algorithms allows us to review and recommend **high-security** features for the most sensitive data.

We realize that even the most carefully protected application can eventually fall victim to an expert hacker, when given enough time. Therefore, it is important to have several forms of defense against an intruder. A good security plan for a network and application should not rely on a single defense mechanism. Many layers of security are required so that subsequent tiers cover holes or flaws in other layers. The security code review can be used to strengthen the application layer, which is a critical component of a **comprehensive** security program.

Our Process

We start by gaining a **detailed understanding** of the application architecture. After meeting with key technical personnel, our lead code reviewer will understand the deployment architecture, application data flow, and code structure. An application demonstration may also be required to understand the user interface components.

The code review team then performs a walk-through of the source code, focusing on areas most vulnerable to attack. After the review, a **risk assessment** is performed to compile a list of issues with supporting documentation and examples. Project managers and application code developers will be able to use this document to prioritize changes and enhancements to the application. A follow-up meeting is conducted to discuss the issues and possible mitigation strategies.

Once changes are made to the application, a subsequent code review is conducted to **verify the resolutions**. When major software releases occur affecting a reviewed application, the code review team can be engaged to perform a 'delta' review to quickly identify any new issues introduced by the change.

Summary

The risk of being the target of Internet based criminal activity is increasing at an alarming pace. The impact of such an attack can be devastating to even the most established companies and organizations. As more and more business is transacted over the Internet, the need for information security has never been greater.

An information security program is only as strong as its weakest link. If there is a vulnerability to be exploited, a determined criminal will find it. Companies and organizations usually focus all their efforts on securing the network and hardening the production environment. A complete security plan should include a security review of all applications that are available on the Internet. The best approach is to plan for security failures and minimize the impact of such an attack by providing multiple layers of security.

An effective corporate security program is multi-faceted. An application code review based on up to date security coding standards and superior technical experience should be considered a main pillar of a comprehensive strategy to secure corporate assets.

References

FFIEC Information Technology Examination Handbook – Information Security Security Testing

http://www.ffiec.gov/ffiecinfobase/html_pages/infosec_book_frame.htm

Public Law 106-102, 106th Congress, 1st Session

Gramm-Leach-Bliley Act of 1999 Title V Sections 501 and 505(b)

<http://banking.senate.gov/conf/fintl5.pdf>

FDIC FIL-118-2002: Information Technology Examination Procedures

<http://www.fdic.gov/news/news/financial/2002/FIL02118.html>

Office of Thrift Supervision's Memorandum to Chief Executive Officers titled "Privacy Preparedness Check-up"

<http://www.ots.treas.gov/docs/48467.pdf>

Thibodeau, Patrick "Feds Set Financial Security 'Guidelines'".

http://www.computerworld.com/cwi/story/0,1199,NAV47_STO56645,00.html

National Standards to Protect the Privacy of Personal Health Information

<http://www.hhs.gov/ocr/hipaa>