Securing E-Commerce: A Systematic Approach

By Anup K. Ghosh, Ph.D.
Research Scientist, Reliable Software Technologies
www.rstcorp.com/~anup
aghosh@rstcorp.com

Anup K. Ghosh is a Research Scientist with Reliable Software Technologies (http://www.rstcorp.com). His research focus is in developing and applying software analysis techniques to problems in computer security. Dr. Ghosh is a principal investigator on research grants from DARPA and Rome Laboratory.

Dr. Ghosh is a noted speaker, consultant, and author on e-commerce security. He has recently completed a book on E-Commerce Security to be published by John Wiley & Sons in January 1998.

Introduction

Electronic commerce, or simply e-commerce, is changing the way in which banks and consumers interact and transact. E-commerce provides consumers the ability to bank, invest, purchase, distribute, communicate, explore, and research from virtually anywhere an Internet connection can be obtained.

Given the explosive growth of the Internet, most e-commerce providers are migrating from proprietary networks and dial-up servers to the Internet in order to capture larger market shares. The World Wide Web, or simply the Web, has become the vehicle of choice for conducting commerce over the Internet because of the user-friendly and rich multi-media interface provided by Web browsers.

The vast growth potential for e-commerce in the banking and financial services industry is tempered by legitimate concerns over the security of such a system. Most diners are not too concerned about the possibility of a waiter keeping an imprint of their credit card number. Similarly, most of us feel comfortable about giving our credit card numbers over the phone to an operator. Why should e-commerce be any different? The answer lies in the scale by which fraud or theft can be perpetrated by flaws in the software systems that facilitate e-commerce transactions. The very nature of computing has the ability to amplify many-fold the effect of a simple error in e-commerce software into large-scale fraud, theft, or security intrusions. A simple error in configuring a commerce site's Web server can lead to the compromise of thousands of credit card numbers which can be quickly and widely distributed.

A recent criminal case illustrates this vividly [1]. Carlos Felipe Salgado Jr. pleaded guilty to have been paid $260,000 in an FBI sting for a diskette containing personal information for over 100,000 credit-card holders. The data was allegedly obtained by Salgado hacking into company databases through the Internet. To protect e-commerce systems from these types of abuses, the systems must be secured systematically.

Securing e-commerce must occur on four fronts: (1) securing the Web clients, (2) securing the data transaction, (3) securing the Web server, and (4) securing the network server operating system. To date only the data transaction protocols have gained recognition and development of secure properties. The security of e-commerce systems, though, are only as strong as their weakest component. A failure to secure any one of these four components of electronic commerce may result in the entire system being insecure. If one component is much more secure than others (e.g., the data transaction protocol versus the network servers), then criminals will attack the weakest component (the path of least resistance).

The benefits of providing goods and services over the Internet are immediately apparent. However, placing a server on the Internet also opens the potential for malicious criminals to break into systems, steal files, deny service and possibly destroy the host systems. Erecting firewalls can prevent attacks against internal computer systems (at least initially); however, firewalls can only provide trivial security assurance against data-driven attacks through the Web.

This article highlights critical vulnerabilities in Web security that providers of e-commerce will find invaluable. First, the security issues for banks and other providers of e-commerce have in using the Internet and the Web are discussed. These issues include: setting up and maintaining a secure Web server, vulnerabilities in web servers, and the dangers of CGI scripts and Web applications in general. Also addressed are the client-side security issues in e-commerce transactions for consumers as well as for employees who use the Web. Security and privacy breaches are a concern when using commercial Web browsers, downloading programs, viewing images, and surfing to Web pages with active content applications. Future articles will address the data transaction security and network server operating system security.

Web Server Vulnerabilities

What are the security issues that companies must be concerned about in using the Web for electronic commerce? First, the setup and configuration of a Web server can be complex and the security implications of a misconfigured server are severe. Take as an example a system administrator who installs and configures a Web server. The system administrator knows that the server must start up as the super user in order to listen to the privileged HTTP port. Without necessarily thinking of the security implications, the system administrator sets the executing privilege of the Web server to the super user. Now, any actions the server takes will have the weight and privilege of the super user. So, if an attacker is able to subvert the server, the attacker will now have super user privileges.

Flaws, shortcomings, or even features in a Web server can provide a gateway for a malicious intruder to break into corporate systems. The Web server is responsible for accepting and responding to requests over the Internet---similar to other network programs which allow users to remotely log into systems. However, the range of functions handled by the Web server is quite large. An axiom of software development is that the more complex the the software, the more likely flaws exist in the software code.

Security professionals are now beginning to recognize and embrace the idea that most security breaches are made possible by flaws in software code. As an example, the HTTPd Web server version 1.4 released from the National Center for Supercomputing Applications (NCSA), which is popularly used at many sites, contained a software flaw that has been a favorite target of many computer crackers [2] . The flaw is in a software routine that is intended to remove possibly malicious input characters in Web server requests. However, when the routine was coded, an ASCII character was omitted from the list of possibly malicious input. This particular character can be used in a simple attack that enables an intruder to execute arbitrary commands on the server. Given this ability, a hacker may retrieve files, write files, and possibly erase files, depending on the privilege with which the Web server is executing. A patch for this problem has since been released; however, the extent to which the vulnerability has been patched in installed versions is unknown.

Web Client Vulnerabilities

Equally important to e-commerce security is the security of client-side software, specifically Web clients. Active content applications such as Java applets, ActiveX controls, JavaScripts, VBScripts, browser plug-ins, and e-mail attachments all pose potential security and privacy hazards for e-commerce end-users.

The first issue companies must wrestle with is whether or not to trust the Web browser itself. Most browsers are given the privilege to execute programs locally, to write to user disks, to upload and download files and programs from the Internet. Since the source code is usually not distributed with the browser, the consumer must trust that the browser software is not performing any malicious actions such as corporate espionage on a file system. Often times, when installing the software, the user must agree not to hold the browser vendor responsible for any damages resulting from use of the browser. Netscape Navigator versions 2.x, 3.x, and 4.1 as well as the Internet Explorer versions 3.x and 4.0 browsers have all had serious flaws that have permitted complete security violations.

Beyond the issue of the browser source itself, companies must be concerned with the features that many browsers provide. The most popular browsers come with options for plug-ins that automatically execute files viewed from remote Web sites. Certainly, this provision makes surfing the Web interesting as far as multimedia presentations; however, executing an untrusted application opens the door for malicious attacks. Perhaps the most popular form of active content available on the Internet is Java applets. When viewing a Web page which has a Java applet attached, the Java applet is downloaded to the client's disk and automatically executed unless this default feature is disabled in the browser. While Java was designed with security measures to prevent unauthorized access to client file systems, this security model has been repeatedly violated [3]. JavaScript has also been shown to contain very serious security holes in previous releases. Corporate users should not download active content unless the source is trusted---and even then, no assurance of security is provided.

In order for corporations to begin to address the security concerns of Web browsing, a security policy must be established and enforced at corporate sites regarding downloading files from the Internet. It is easily conceivable that an employee could unknowingly download a virus, a malicious program that opens a backdoor in the system, or even images which have programs encoded in them that are executed once downloaded. This malicious use of images to store programs is a focus of a field of research called steganography. Java security is expected to improve over the long term, but until the security issues are resolved, it is safest to disable Java and Javascript unless you are viewing trusted applets. System-wide filtering solutions are also available for preventing executable content from being downloaded over the Internet.

Conclusions

The Internet today is a vast frontier of unknown elements including new types of software, new discoveries of security flaws, and unfriendly neighbors. The most secure technical solution to preventing attacks launched from the Internet is to unplug the network from the computer. This solution is not viable in today's business climate. Rather, the components that comprise e-commerce systems must be adequately secured.

Two components of e-commerce that are often overlooked in security are the network server software and the Web clients. For mis-configured servers (mail, news, Web, FTP, and others), breaking into a site becomes as simple as following a recipe (usually published in underground sites). Armed with the facts about security, corporate MIS managers and system administrators can begin to make appropriate decisions to secure e-commerce.

References

[1] P.G. Neumann, "Carlos Salgado Jr. pleads guilty" *RISKS Digest*, Vol. 19, Issue 34, August 26, 1997.

[2] CERT Advisory 96.06, "cgi example code", URL: ftp://info.cert.org/pub/cert_advisories>.

[3] G. McGraw and E. Felten, *Java Security: Hostile Applets, Holes, and Antidotes*, John Wiley & Sons, New York, 1996.

[Home]