Chapter 15
Developing Security Enabled Applications for Web Commerce

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

ABSTRACT

As more and more applications find their way to the World Wide Web, security concerns have increased. Web applications are by nature somewhat public and therefore vulnerable to attack. Today it is the norm to visit Web sites where logins and passwords are required to navigate from one section of the site to another. This is much more so required in a Web application where data is being manipulated between secure internal networks and the Internet. Web applications, no matter what their functions are, should not exchange data over the Internet unless it is encrypted or at least digitally signed. Security should be extended to the private-public network borders to provide the same authentication, access control, and accounting services that local area network (LAN) based applications employ. The most widely used method of Web application security today is Private Key Infrastructure (PKI). Various examples of PKI implementations are examined.

INTRODUCTION

We explore toolkits useful for building secure Web and e-mail applications, specifically Pharos Technologies' security toolkits, which are used to create applications that run the gamut of security methods. The main message of this chapter is that successfully developed Web applications must also be security-conscious Web applications. This is not only true at the application code level; it is also true at the Web site and server levels as well. Webmasters as well as developers need to be more concerned with security of their systems as hackers continue to come up with new ways to disable Web sites and dismantle Web applications.

DOI: 10.4018/978-1-5225-3422-8.ch015

BENEFITS OF USING SECURITY-ENABLED APPLICATIONS

On first inspection, one would say the reasons why we need security built into applications are ridiculously obvious, but principles this essential are worth reviewing:

- *A decent hacker can exploit weaknesses in any application after he is familiar with the language it was created in*. Take, for instance, the Melissa virus or other viruses that affect Microsoft Office applications. A hacker with a good knowledge of Visual Basic for Applications (VBA),Visual Basic, or Visual C++ could wreak havoc (as has already been demonstrated by the Melissa virus) on systems running MS Office. Security here would serve to at least warn the unsuspecting user that the e-mail attachment they are about to open has macros that are potentially dangerous and would offer to disable the macros, thereby rendering the hacker's code useless.
- *Not everyone in your organization needs access to all information*. Security in this case would not allow access to a user unless she can prove that she should be granted access by her identity. Data should be protected from undesirable eyes at all times, especially data that traverses the Internet. E-mail applications that are capable of securing their data via encryption, or corporate Intranet applications that use certificates, go a long way to preventing information leaks. For example, a corporate Intranet site might be a good place for keeping employee information. Not everyone in the Human Resources department should have access to all the information, not to mention that everyone in the company shouldn't either. Building an Intranet employing PKI standards for access control would give access to only those people that need to view or manipulate this information.
- *A means of authentication, authorization, and nonrepudiation is an integral part of securing your applications, both on the Web and within your private networks*.

Applications with built-in security methods make it easier to safely conduct business on any network. In addition, knowing how to easily secure applications make it simpler to build an entire security infrastructure around them. Many types of major security breaches can be avoided if Web administrators and developers consider more than just the functionality of their systems.

TYPES OF SECURITY USED IN APPLICATIONS

As e-commerce gains in popularity, and more and more data is transferred across the Internet, application security becomes essential (Russell, 2001; Bhasin, 2003). We discuss the transferring of data over and over again throughout this chapter, and it is important to note that we are not just referring to credit card information; data can be much more in-depth and private than that. When we discuss data transfer, think of private healthcare information or insurance information. Or think in terms of proprietary data that deserves the most secure transmissions.

Because of the different levels of security that are needed at times, and because security is needed at more than just a network level, this section delves into the depths of security that is used at the application level. We discuss the use of digital signatures: what are they and when are they used? We also take a close look at Pretty Good Privacy (PGP) and its use within e-mail. We all realize the vital role that e-mail plays in both business and personal lives today; given that, we should probably all understand how security works within the e-mail that we have all grown so intimate with. Following along the same lines,