E-COMMERCE SECURITY STRATEGIES

Munteanu Alin

"Tibiscus" University of Timisoara, Faculty of Economics, 1/A Daliei Street, 300558, Timisoara, Romania, Phone: +40-256-202931, E-mail: a_munteanu@yahoo.com

This article presents an overview of security and privacy concerns based on the author experiences as testing a few applications developers. It explores the current state of e-Commerce applications and describes techniques that can make your online site or online shopping experience more secure.The aplications are business middleware that accelerates the development of any business transaction-oriented application, from the smallest online retailer to B2B portals, to supply chain management applications and provides an integrated platform that runs both their customer facing online shopping sites, and their internal distributor or supplier portals.

Key words: e-commerce, Internet, security

Introduction

The applications for e-commerce are business middleware that accelerates the development of any business transaction-oriented application, from the smallest online retailer to B2B portals, to supply chain management applications. For many clients, this aplications provide an integrated platform that runs both their customer facing online shopping sites, and their internal distributor or supplier portals as shown in Figure 1.

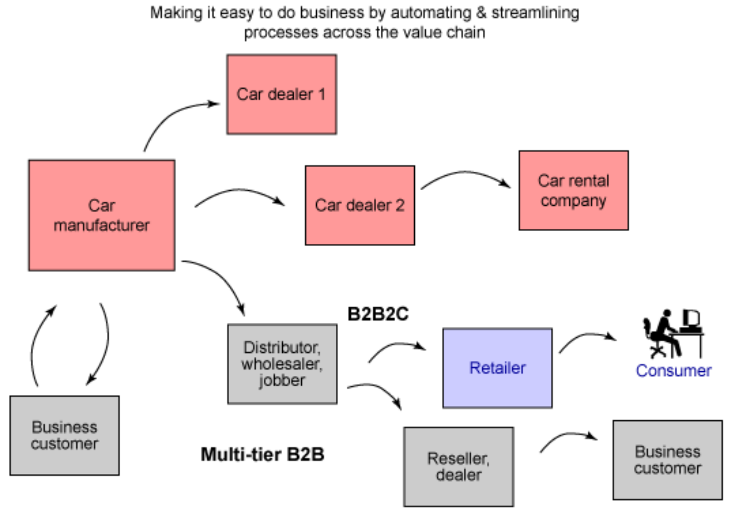

Figure 1. Common applications business model

E-commerce refers to the exchange of goods and services over the Internet. All major retail brands have an online presence, and many brands have no associated bricks and mortar presence. However, e-Commerce also applies to business to business transactions, for example, between manufacturers and suppliers or distributors.

Security overview

A secure system accomplishes its task with no unintended side effects. Using the analogy of a house to represent the system, you decide to carve out a piece of your front door to give your pets' easy access to the outdoors. However, the hole is too large, giving access to burglars. In the software industry, security has two different perspectives. In the software development community, it describes the security features of a system. Common security features are ensuring passwords that are at least six characters long and encryption of sensitive data. For software consumers, it is protection against attacks rather than specific features of the system. Your house may have the latest alarm system and windows with bars, but if you leave your doors unlocked, despite the number of security features your system has, it is still insecure. Hence, security is not a number of features, but a system process. The weakest link in the chain determines the security of the system. In this article, we focus on possible attack scenarios in an e-commerce system and provide preventive strategies, including security features, that you can implement.

Security has three main concepts: confidentiality, integrity, and availability. Confidentiality allows only authorized parties to read protected information. For example, if the postman reads your mail, this is a breach of your privacy. Integrity ensures data remains as is from the sender to the receiver. If someone added an extra bill to the envelope, which contained your credit card bill, he has violated the integrity of the mail. Availability

المنارة للاستشارات
www.manaraa.com

ensures you have access and are authorized to resources. If the post office destroys your mail or the postman takes one year to deliver your mail, he has impacted the availability of your mail.

In a typical e-commerce experience, a shopper proceeds to a Web site to browse a catalog and make a purchase. This simple activity illustrates the four major players in e-commerce security. One player is the shopper who uses his browser to locate the site. The site is usually operated by a merchant, also a player, whose business is to sell merchandise to make a profit. As the merchant business is selling goods and services, not building software, he usually purchases most of the software to run his site from third-party software vendors. The software vendor is the last of the three legitimate players. The attacker is the player whose goal is to exploit the other three players for illegitimate gains.

The attacker can besiege the players and their resources with various damaging or benign schemes that result in system exploitation. Threats and vulnerabilities are classified under confidentiality, integrity, and availability. A threat is a possible attack against a system. It does not necessarily mean that the system is vulnerable to the attack. An attacker can threaten to throw eggs against your brick house, but it is harmless. A vulnerability is a weakness in the system, but it is not necessarily known by the attacker.

Security features

While security features do not guarantee a secure system, they are necessary to build a secure system. Security features have four categories:

- authentication: Verifies who you say you are. It enforces that you are the only one allowed to logon to your Internet banking account;
- authorization: Allows only you to manipulate your resources in specific ways. This prevents you from increasing the balance of your account or deleting a bill;
- encryption: Deals with information hiding. It ensures you cannot spy on others during Internet banking transactions;
- auditing: Keeps a record of operations. Merchants use auditing to prove that you bought a specific merchandise.

Password policies are enforced for shoppers and internal users. A sample password policy, defined as part of the Federal Information Processing Standard (FIPS), is shown in the table below.

Tabel 1

Policy	Value
Account lockout threshold	6 attempts
Consecutive unsuccessful login delay	10 seconds
Matching user ID and password	N (no, they cannot match)
Maximum occurrence of consecutive characters	3 characters
Maximum instances of any character	4 instances
Maximum lifetime of passwords	180 days
Minimum number of alphabetic characters	1 alphabetic character
Minimum number of numeric characters	1 numeric character
Minimum length of password	6 characters
Reuse user's previous password	N (no, cannot be reused)

Source: Howard M., LeBland D., Writing Secure Code, Second Edition, Microsoft Press, 2003

Site development best practices

Security policies and standards

There are many established policies and standards for avoiding security issues. However, they are not required by law. Some basic rules include:

المنارة للاستشارات
www.manaraa.com

- Never store a user's password in plain text or encrypted text on the system. Instead, use a one-way hashing algorithm to prevent password extraction.
- Employ external security consultants (ethical hackers) to analyze your system.
- Standards, such as the Federal Information Processing Standard (FIPS), describe guidelines for implementing features. For example, FIPS makes recommendations on password policies.
- Ensure that a sufficiently robust encryption algorithm, such as triple DES or AES, is used to encrypt all confidential information stored on the system.
- When developing third-party software for e-commerce applications, use external auditors to verify that appropriate processes and techniques are being followed.

Recently, there has been an effort to consolidate these best practices as the Common Criteria for IT Security Evaluation (CC). CC seems to be gaining attraction. It is directly applicable to the development of specific e-commerce sites and to the development of third party software used as an infrastructure in e-commerce sites.

Using cookies

One of the issues faced by Web site designers is maintaining a secure session with a client over subsequent requests. Because HTTP is stateless, unless some kind of session token is passed back and forth on every request, the server has no way to link together requests made by the same person. Cookies are a popular mechanism for this. An identifier for the user or session is stored in a cookie and read on every request. You can use cookies to store user preference information, such as language and currency. This simplifies Web page development because you do not have to be concerned about passing this information back to the server. The primary use of cookies is to store authentication and session information, your information, and your preferences. A secondary and controversial usage of cookies is to track the activities of users.

Cookies marked as secure (storing encrypted data and passing to the user only under SSL) remain the most popular method of providing a secure online experience.

Using an online security checklist

Use this security checklist to protect yourself as a shopper:

- Whenever you logon, register, or enter private information, such as credit card data, ensure your browser is communicating with the server using SSL.
- Do not shop at a site when the browser does not recognize the server's SSL certificate. This check is done by your browser the first time your URL becomes HTTPS for the site. If the certificate is not recognized, then your browser presents a pop-up message to inform you.
- Use a password of at least 6 characters, and ensure that it contains some numeric and special characters (for example, c0113g3).
- Avoid reusing the same user ID and password at multiple Web sites.
- If you are authenticated (logged on) to a site, always logoff after you finish.

Conclusion

This article outlined the key players and security attacks and defenses in an e-commerce system. Current technology allows for secure site design. It is up to the development team to be both proactive and reactive in handling security threats, and up to the shopper to be vigilant when shopping online.

References:

1. Schneier B., Secrets and Lies: Digital Security In A Networked World, John Wiley and Sons, Inc., 2000, p. 97-143
2. Howard M., LeBland D., Writing Secure Code, Second Edition, Microsoft Press, 2003, p. 52-67
3. http://publib.boulder.ibm.com/infocenter/wc56help/index.jsp
4. http://wired-vig.wired.com/news/business/0,1367,34221,00.html
5. http://www-128.ibm.com/developerworks/websphere/zones/commerce
6. Patriciu, V. V., at all., Securitatea comertului electronic, Editura All, 2001, p. 177-193

المنارة للاستشارات
www.manaraa.com

www.manaraa.com