Volume 6, Issue 4, April 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on E-Commerce Security Issues and Solutions

Arvind Sharma
Assistant Professor, Department of Computer Science, DAV College,
Amritsar, Punjab, India

Abstract: Electronic commerce, commonly known as e-commerce or e-business consists of the buying and selling of products or services over electronic systems such as the Internet and other computer networks. The amount of trade conducted electronically has grown extraordinarily with widespread Internet usage. During the e-commerce process crucial business transactions are carried. Even individuals perform online transactions like e-banking and shopping etc. over the internet. It is here that the actual threat grips the mind of every person that is the information passed on the net is secure? While security features do not guarantee a secure system, they are necessary to build a secure system. This paper presents an overview of security and privacy concerns associated with e-commerce and the possible solutions for them.

Keywords: B2B, snooping, sniffing, SSL.

I. INTRODUCTION

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. E-commerce systems are also relevant for the services industry. For example, online banking and brokerage services allow customers to retrieve bank statements online, transfer funds, pay credit card bills, apply for and receive approval for a new mortgage, buy and sell securities, and get financial guidance and information. Electronic commerce that is conducted between businesses is referred to as business-to-business or B2B. B2B can be open to all interested parties (e.g. commodity exchange) or limited to specific, pre-qualified participants (private electronic market). Electronic commerce that is conducted between businesses and consumers, on the other hand, is referred to as business-to-consumer or B2C. This is the type of electronic commerce conducted by companies such as Amazon.com. Online shopping is a form of electronic commerce where the buyer is directly online to the seller's computer usually via the internet. There is no intermediary service. The sale and purchase transaction is completed electronically and interactively in real-time such as Amazon.com for new books. If an intermediary is present, then the sale and purchase transaction is called electronic commerce such as eBay.com.

II. THE CRIMINAL INCENTIVE

Attacks against e-Commerce Web sites are so alarming, they follow right after violent crimes in the news. Practically every month, there is an announcement of an attack on a major Web site where sensitive information is obtained. Why is e-commerce vulnerable? Is e-commerce software more insecure compared to other software? Did the number of criminals in the world increase? The developers producing e-commerce software are pulled from the same pool of developers as those who work on other software. In fact, this relatively new field is an attraction for top talent. Therefore, the quality of software being produced is relatively the same compared to other products. The criminal population did not undergo a sudden explosion, but the incentives of an e-commerce exploit are a bargain compared to other illegal opportunities.

III. ATTACKS

This section describes potential security attack methods from an attacker or hacker.

3.1 Tricking the shopper

Some of the easiest and most profitable attacks are based on tricking the shopper, also known as social engineering techniques. These attacks involve surveillance of the shopper's behavior, gathering information to use against the shopper. For example, a mother's maiden name is a common challenge question used by numerous sites. If one of these sites is tricked into giving away a password once the challenge question is provided, then not only has this site been compromised, but it is also likely that the shopper used the same logon ID and password on other sites.

3.2 Snooping the shopper's computer

Millions of computers are added to the Internet every month. Most users' knowledge of security vulnerabilities of their systems is vague at best. Additionally, software and hardware vendors, in their quest to ensure that their products

are easy to install, will ship products with security features disabled. In most cases, enabling security features requires a non-technical user to read manuals written for the technologist. The confused user does not attempt to enable the security features. This creates a treasure trove for attackers.

3.3 Sniffing the network

In this scheme, the attacker monitors the data between the shopper's computer and the server. He collects data about the shopper or steals personal information, such as credit card numbers. There are points in the network where this attack is more practical than others.

3.4 Guessing passwords

Another common attack is to guess a user's password. This style of attack is manual or automated. Manual attacks are laborious, and only successful if the attacker knows something about the shopper. For example, if the shopper uses their child's name as the password. Automated attacks have a higher likelihood of success, because the probability of guessing a user ID/password becomes more significant as the number of tries increases. Tools exist that use all the words in the dictionary to test user ID/password combinations, or that attack popular user ID/password combinations. The attacker can automate to go against multiple sites at one time.

3.5 Using denial of service attacks

The denial of service attack is one of the best examples of impacting site availability. It involves getting the server to perform a large number of mundane tasks, exceeding the capacity of the server to cope with any other task.

3.6 Using server root exploits

Root exploits refer to techniques that gain super user access to the server. This is the most coveted type of exploit because the possibilities are limitless. When you attack a shopper or his computer, you can only affect one individual. With a root exploit, you gain control of the merchants and all the shoppers' information on the site.

IV. SOLUTIONS

4.1 Education

Your system is only as secure as the people who use it. If a shopper chooses a weak password, or does not keep their password confidential, then an attacker can pose as that user. This is significant if the compromised password belongs to an administrator of the system.

4.2 Personal firewalls

When connecting your computer to a network, it becomes vulnerable to attack. A personal firewall helps protect your computer by limiting the types of traffic initiated by and directed to your computer. The intruder can also scan the hard drive to detect any stored passwords.

4.3 Secure Socket Layer (SSL)

Secure Socket Layer (SSL) is a protocol that encrypts data between the shopper's computer and the site's server. When an SSL-protected page is requested, the browser identifies the server as a trusted entity and initiates a handshake to pass encryption key information back and forth. Now, on subsequent requests to the server, the information flowing back and forth is encrypted so that a hacker sniffing the network cannot read the contents.

4.4 Server firewalls

A firewall is like the moat surrounding a castle. It ensures that requests can only enter the system from specified ports, and in some cases, ensures that all accesses are only from certain physical machines.

4.5 Intrusion detection and audits of security logs

One of the cornerstones of an effective security strategy is to prevent attacks and to detect potential attackers. This helps understand the nature of the system's traffic, or as a starting point for litigation against the attackers.

4.6 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.

V. CONCLUSION

This paper 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] Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012

[2] Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences – 2002

[3] Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8 No.5, May 2008

[4] W. Jeberson, Prof. (Col.). Gurmit Singh. "Analysis of Security Measures Implemented on G2C Online Payment Systems in India" MIT International Journal of Computer Science & Information Technology Vol. 1 No. 1 Jan. 2011

[5] Pradnya B. Rane, Dr. B.B.Meshram. "Transaction Security for Ecommerce Application" IJECSE -ISSN- 2277-1956. 2012

[6] Mohanad Halaweh, Christine Fidler - " Security Perception in Ecommerce: Conflict between Customer and Organizational Perspectives" Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 443 – 449, ISBN 978-83-60810-14-9- 2008-IEEE

