Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 8, (Special Issue) June-2019, ISSN 2230-7540

Security Issues in E-Commerce

Dr. Anupam Jain*

Lecturer ABST and Head, Department of Commerce, LBS PG College, Tilak Nagar, Raja Park, Jaipur, Rajasthan

Abstract – This paper deals with the security related issues in E-Commerce for the online users. It explains the basic scenario of E-commerce working and explains the security concept in online transactions. It also explains the security methods used by E-business sites. It also explains the most frequently questions raised by the users and provides the solutions for their queries.

Keywords: Digital Signatures, Firewalls, Secure Socket Layers and Secure Electronic Transactions.

----------X----------

INTRODUCTION

In our society, today, more and more people are using the technology for their routine jobs. Computers has changed the every way of life and they are now become necessity for everyone. In today's era, Computer knowledge is essential. Internet has made the communication very fast and no business can flourish today without computers and internet. E-commerce has changed the scenario of the business but security is the major issue in e-commerce. For e-commerce, business must create a website that promotes the products, obtain an Internet address, hire space on a web server, upload web pages, add a payment system and then use various advertising services to get their site noticed. Websites can be very ambitious, with eye-catching graphics, animation, sound, database search systems, customer recognition and many other features.

Electronic Commerce (E-Commerce) has become a buzzword for business over the past few years, with increased awareness about the use of computer and communication technologies to simplify business procedures and increase efficiency. E-Commerce simply means selling over the Internet — goods, services, information and whatever. The E-commerce makes the commercial transactions online and allows users to perform their commercial activities from anywhere and anytime. So E-Commerce comprises core business processes of buying, selling goods, services and information over the internet. The E-Commerce is really doing well. Transactions are also conducting on mobiles.

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.

SECURITY OVERVIEW

A secure system accomplishes its task with no unintended side effects. Using the analogy of a house to represent the system, we decide to carve out a piece of our front door to give our pets' easy access to the outdoors. However, the hole is too large, giving access to burglars. We have created an unintended implication and therefore, an insecure system.

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. Our house may have the latest alarm system and windows with bars, but if we leave our doors unlocked, despite the number of security features in our 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 we 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 our mail, this is a breach of our 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 ensures you have

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

REQUIREMENTS FOR SECURED TRANSACTIONS

The basic principles for customer **security** for any e-Commerce system must meet the following requirements:-

a) **Privacy** of information must be kept from unauthorized users. Privacy is handled by encryption. In PKI (public key infrastructure) a message is encrypted by a public key, and decrypted by a private key. The public key is widely distributed, but only the recipient has the private key.

b) **Integrity** of message must not be distorted.

c) **Authentication** process must be completed i.e. sender and receiver must verify their identities to each other. For authentication the encrypted message is encrypted again (proving the identity of the sender, because only the sender has the particular key), but this time with a private key. Such procedures form the basis of RSA (used by banks and governments) and PGP (Pretty Good Privacy, used to encrypt emails).

d) **Proof** is needed that the message was definitely acknowledged.

PROBLEMS WITH E-COMMERCE

The problem with E-Commerce is that the area of covering is very wide. Additionally, E-Business must protect against the unknown. There are no such widely acceptable and standard policies that make the security possible. Customers are still having fear to pass their credit card numbers online. They see the products online and then purchase them from the retailer. Reports of holes in companies' e-commerce systems could convince even the most rational person that thieves are prowling every corner of the Web, waiting to steal victims' credit card numbers, personal data and other sensitive information.

The tremendous increase in online transactions has been accompanied by an equal rise in the number and type of attacks against the security of online payment systems.

The following problems may arise due to E-Commerce:

THE PLAYERS

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. Figure 2 illustrates the players in a shopping experience.

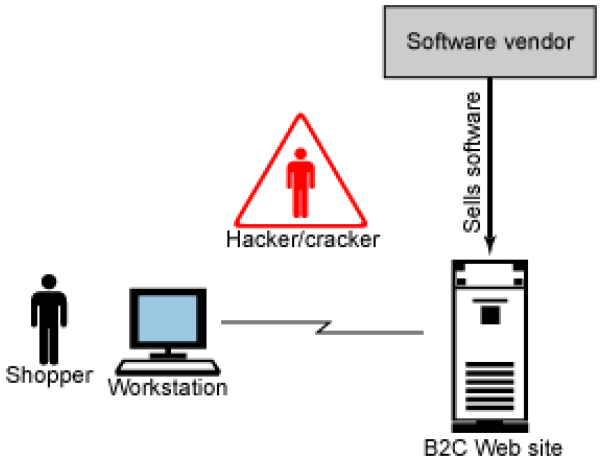

Figure 1. The players

POINTS THE ATTACKER CAN TARGET

As mentioned, the vulnerability of a system exists at the entry and exit points within the system. Figure 2 shows an e-Commerce system with several points that the attacker can target:

- Shopper
- Shopper' computer
- Network connection between shopper and Web site's server
- Web site's server
- Software vendor

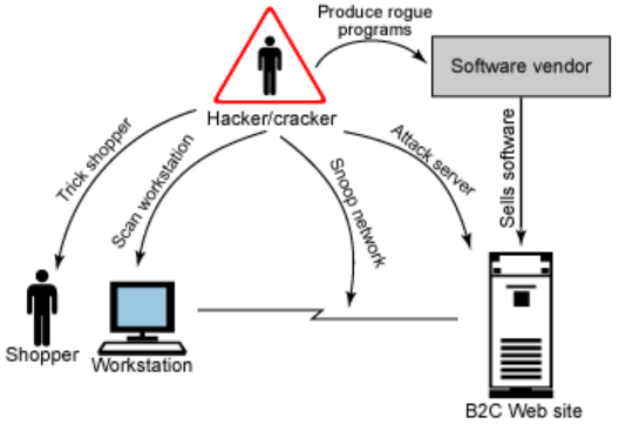

Figure 2. Points the attacker can target

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. If the attacker sits in the middle of the network, then within the scope of the Internet, this attack becomes impractical. A request from the client to the server computer is broken up into small pieces known as packets as it leaves the client's computer and is reconstructed at the server. The packets of a request are sent through different routes. The attacker cannot access all the packets of a request and cannot decipher what message was sent.

Take the example of a shopper in Toronto purchasing goods from a store in Los Angeles. Some packets for a request are routed through New York, where others are routed through Chicago. A more practical location for this attack is near the shopper's computer or the server. Wireless hubs make attacks on the shopper's computer network the better choice because most wireless hubs are shipped with security features disabled. This allows an attacker to easily scan unencrypted traffic from the user's computer.

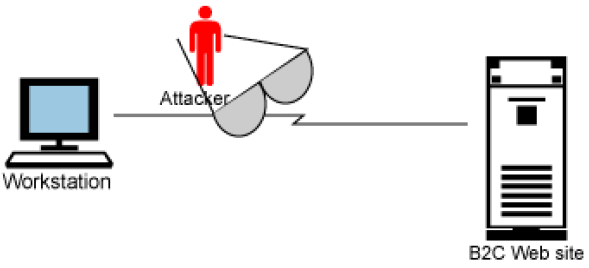

Figure 3. Attacker sniffing the network between client and server

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. For example, if everyone in a large meeting asks us our name all at once, and every time you answer, they ask you again. You have experienced a personal denial of service attack. To ask a computer its name, you use ping. You can use ping to build an effective DoS (Denial of Service) attack. The smart hacker gets the server to use more computational resources in processing the request than the adversary does in generating the request.

Distributed DoS is a type of attack used on popular sites, such as Yahoo!®. In this type of attack, the hacker infects computers on the Internet via a virus or other means. The infected computer becomes slaves to the hacker. The hacker controls them at a predetermined time to bombard the target server with useless, but intensive resource consuming requests. This attack not only causes the target site to experience problems, but also the entire Internet as the number of packets is routed via many different paths to the target.

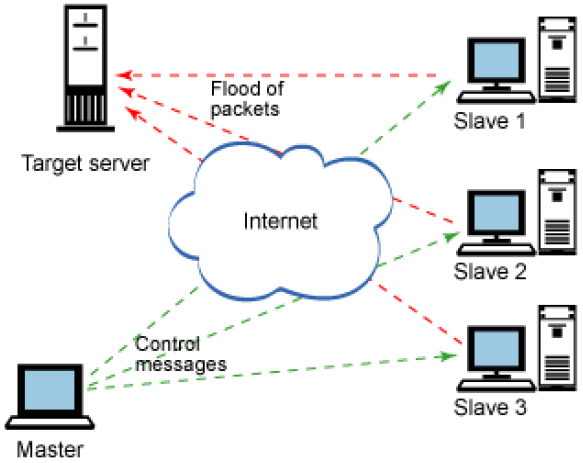

Figure 4. Denial of service attacks

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.

USING KNOWN SERVER BUGS

The attacker analyzes the site to find what types of software are used on the site. He then proceeds to find what patches were issued for the software. Additionally, he searches on how to exploit a system without the patch. He proceeds to try each of the exploits. The sophisticated attacker finds a weakness in a similar type of software, and tries to use that to exploit the system. This is a simple, but effective attack. With millions of servers online, what is the probability that a system administrator forgot to apply a patch?

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. There are two main types of root exploits: buffer overflow attacks and executing scripts against a server.

In a buffer overflow attack, the hacker takes advantage of specific type of computer program bug that involves the allocation of storage during program execution. The technique involves tricking the server into execute code written by the attacker.

The other technique uses knowledge of scripts that are executed by the server. This is easily and freely found in the programming guides for the server. The attacker tries to construct scripts in the URL of his browser to retrieve information from his server. This technique is frequently used when the attacker is trying to retrieve data from the server's database.

DEFENSES AND REMEDIES

Despite the existence of hackers and crackers, e-Commerce remains a safe and secure activity. The resources available to large companies involved in e-Commerce are enormous. These companies will pursue every legal route to protect their customers. Figure 5 shows a high-level illustration of defenses available against attacks.

DIGITAL SIGNATURES

Digital signatures meet the need for authentication and integrity. A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is not change. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any type of message, whether it is encrypted or not, so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

SECURE SOCKET LAYERS

Information sent over the Internet commonly uses the set of rules called TCP/IP (Transmission Control Protocol / Internet Protocol). The information is broken into packets, numbered sequentially, and an error control attached. Each Individual packet is sent by different routes. TCP/IP re-assembles them in order and resubmits any packet showing errors. SSL uses PKI and digital certificates to ensure privacy and authentication.

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.

A common technique is to setup a demilitarized zone (DMZ) using two firewalls. The outer firewall has ports open that allow ingoing and outgoing HTTP requests. This allows the client browser to communicate with the server. A second firewall sits behind the e-Commerce servers. This firewall is heavily fortified, and only requests from trusted servers on specific ports are allowed through. Both firewalls use intrusion detection software to detect any unauthorized access attempts.

Another common technique used in conjunction with a DMZ is a honey pot server. A honey pot is a resource (for example, a fake payment server) placed in the DMZ to fool the hacker into thinking he has penetrated the inner wall. These servers are closely monitored, and any access by an attacker is detected.

Firewalls (software or hardware) protect a server or a network and an individual PC from attack by viruses and hackers. Equally important is protection from mischievousness or carelessness within the system, many companies are using the Kerberos protocol, which uses symmetric secret key cryptography to restrict access to authorized employees.

SET (SECURE ELECTRONIC TRANSACTION)

SET is developed by Visa and MasterCard; SET uses PKI for privacy, and digital certificates to authenticate the three parties: merchant, customer and bank. More importantly, sensitive information is not seen by the merchant, and is not kept on the merchant's server.

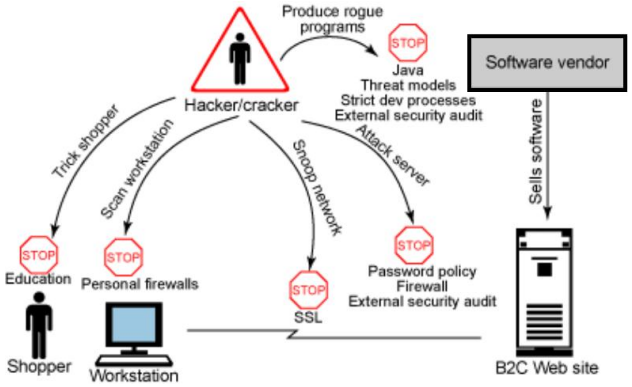

Figure 5. Attacks and their defenses

Frequently asked questions and answers

The most frequently asked e-commerce security questions are -

a) *What happens if someone steals a Customer's credit/debit card number?*

All major credit/debit card companies or banks provide the consumer protection. In most cases, this means the consumer is liable for a bare minimum amount as long as they report the unauthorized use in a timely manner. The consequences can be far worse for the business from which the number was stolen — such incidents can ruin a company's reputation and possibly expose it to legal liability.

b) Is it possible that a cyber-thief can hack a customer's credit/debit card number on the Web?

A properly configured e-commerce system makes it almost impossible to hack a customer's credit/debit card number. The customer's browser uses a secure connection to encrypt their credit card number and other information before it's sent; this data will remain encrypted once it's on the merchant's server. Even if thieves hack this encrypted data, they have no way to read it.

c) *What about the flaws in e-commerce systems that are reported by the Newspapers and TV?*

These problems are the real, sometimes it may be serious. Almost all of these flaws, however, involve incomprehensible, extremely advanced technical knowledge of the system. Most of them are discovered by computer researchers who report the problems to software companies even before they appear in the media. E-commerce hosting firm will carefully check the latest bugs and security flaws, and they'll fix potential problems before an intruder has the chance to exploit them.

d) *E-commerce sites might not always fix these security flaws or even they don't know about it.*

That might be true, computer security requires constant watchfulness, and administrators must know about the problems and ways to fix them. That's why it's important for a business to use a reputed, experienced e-commerce provider. Small firms don't have the expertise to handle these problems on their own.

Security is a worrisome, costly and complicated business, but a single lapse can be expensive in terms of financial loss, records and reputation. Don't wait for disaster to strike, but stay practical by, employing a security expert where necessary.

REFERENCES:

1. Basics of E-Commerce, Legal and Security issues, PHI
2. E-Commerce: Fundamentals and Applications: Chan, Lee, Dillon and Chang, (Wiley India)
3. E-Security and You : Sandeep Oberoi (TMH)
4. E-Commerce Developer's Guide : Noel Jerke, (BPB)
5. Joseph P.T., & Chapter S.J. (2016). History of E-commerce and Indian Business context E– Commerce: An Indian Perspective, Prentice Hall of India Pvt Ltd, India.
6. http://conerlyconsulting.com/ecommerce.pdf
7. Douglas Goldstein (2017). E-Healthcare: Harness the Power of Internet, E-Commerce & E-Care with CDROM, Jones and Bartlett Publishers.
8. Murthy C.S.V. (2017). E-commerce concepts, Models, Strategies, Himalaya Publishing House.
9. Udayan K. Mandvia (2016). Agricultural Marketing and Information Technology, Globalization & Agricultural Marketing, Excel India.

10. Azam (2018). E-Commerce Taxation and Cyberspace Law, Virginia Journal of Law & Technology, Vol. 12, pp. 29.

11. Sheeja V.S., Naveen M.V., Prasad N.R., Sathibabu T. & Murali Krishna R. (2018). Role of E-marketing in Pharmaceutical Business, Pharmanest - An International Journal of Advances in Pharmaceutical Sciences, 2(pp. 2-3), March-June 2018, www.pharmanest.net

12. Dewan, R., Seidmann, A. (2001, June). Current Issues in e-Banking. Communications of the ACM, 44(5), pp. 31-32.

13. Engen, J. (2000). Financial Funnel. Banking Strategies, 76(6), pp. 64–72.

14. Fonseca, J. (2001). Complexity and Innovation in Organisations. Routledge: London.

15. Growth of Electronic Commerce. International Journal of Electronic Commerce, Winter, 4(2), pp. 25-43.

16. Han, K. S., & Noh, M. H. (1999-2000). Critical Failure Factors That Discourage the Growth of Electronic Commerce. International Journal of Electronic Commerce, Winter, 4(2), pp. 25-43.

17. Journal of Financial Services Marketing, 6(4), pp. 323-332.

Websites

1. http://www.securityfocus.com

2. http://www.ecommerce-digest.com

3. http://www.ecombusiness.com

4. http://www.card-media.co.uk/security.htm

5. http://www.thewebbrains.com/ ecommerce_solutions.htm

Corresponding Author

Dr. Anupam Jain*

Lecturer ABST and Head, Department of Commerce, LBS PG College, Tilak Nagar, Raja Park, Jaipur, Rajasthan