Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 1, January 2017, pg.100 – 102

Study on E-Commerce Security Issues and Solutions

Dr. Pranav Patil
Assistant Professor, Department of Computer Science, M. J. College, Jalgaon, Maharashtra, India

Abstract: Electronic commerce, usually called e-commerce or e-business consists of the shopping for and commerce of product or services over electronic systems like the web and different computer networks. The number of trade conducted electronically has full-grown terribly with widespread web usage. During the e-commerce method crucial business transactions are carried. Even people perform on-line transactions like e-banking and looking etc. over the web. It is here that the particular threat grips the mind of each person who is that the data passed on Infobahn is secure? Whereas security measures do not assurance a secure system, they are required to create a secure system. This paper presents a summary of security and privacy issues related to e-commerce and also the possible solutions for them.
Keywords: B2B, snooping, sniffing, SSL.

1. Introduction

E-Commerce introduces to the trade of products and services over the web. All major retail brands have a web presence, and lots of brands haven't any associated bricks and mortar presence. However, e-commerce additionally applies to business to business transactions, as an example, between makers and suppliers or distributors. E-commerce systems are relevant for the services trade. As an example, on-line banking and brokerage services enable customers to retrieve bank statements on-line, transfer funds, pay MasterCard bills, apply for and receive approval for a replacement mortgage, get and sell securities, and obtain money steerage and data. Electronic commerce that is conducted between businesses is mentioned as business-to-business or B2B. B2B are often hospitable all interested parties (e.g. trade goods exchange) or restricted to particular, pre-qualified participants (personal electronic market). Electronic commerce that is conducted between businesses and customers, on the opposite hand, is mentioned as business-to-consumer or B2C. This is often the kind of electronic commerce conducted by compacts like, flip cart, Amazon.com. On-line seeking could be a type of electronic commerce wherever the customer is directly on-line to the dealer's computer usually using the web. There is no inter-mediator service. The sale and buy dealings are completed electronically and interactively in period of time like Amazon.com for brand spanking new books. If an intermediates is gift, then the sale and buy dealings is named electronic commerce like eBay.com.

2. The Criminal Incentive

Attacks against e-Commerce websites are therefore horrible; they follow right once violent crimes within the news. Much monthly, there is an announcement of an attack on a serious site wherever sensitive data is acquired. Why is e-commerce at risk? Is e-commerce software system additional insecure compared to different software system? Did the quantity of criminals within the world increase? The developers manufacturing e-commerce software system are force from identical pool of developers as those that work on different software. In fact, this comparatively new field is an attraction for prime talent. Therefore, the standard of software system being made is comparatively identical compared to different product. The criminal population did not bear a unexpected explosion, however the incentives of an e-commerce exploit are a discount compared to different prohibited opportunities.

3. ATTACKS

This part describes potential protection attack ways from an assaulter or hacker.

3.1 Tricking the consumer: Some of the simplest and most profitable attacks are supported tricking the consumer, additionally referred to as social engineering methods. These attacks grip surveillance of the shopper's behavior, gathering data to use against the consumer. As an example, a mother's last name may be a common challenge question utilized by varied sites. If one in every of these sites is tricked into giving freely a password once the challenge question is provided, then not only has this web site been give and take, however it is additionally probably that the consumer used identical logon ID and password on alternative sites.

3.2 Inquiring the consumer's computer: Lacks of computers are additional to the web monthly. Most users' data of security vulnerabilities of their systems is imprecise at the best. In addition, code and hardware vendors, in their quest to make sure that their merchandise are simple to put in, can ship merchandise with safety features disabled. In most cases, enabling safety features needs a non-technical user to scan manuals written for the engineer. The confused user doesn't plan to alter the safety options. This creates a treasure for attackers.

3.3 Sniffing the network: In this theme, the aggressor monitors the information between the shopper's computer and therefore the server. He collects information concerning the consumer or steals personal information, like master card numbers. There are points within the network wherever this attack is additional sensible than others.

3.4 Guessing passwords: General attack is to guess a user's secret word. This variety of attack is manual or automatic. Manual attacks are toilsome, and only self-made if the attacker is aware of one thing concerning the consumer. As an example, if the consumer uses their child's name because the password. Automatic attacks have a better probability of success, as a result of the likelihood of guess a user ID/password becomes a lot of vital because the range of tries will increase. Tools exist that use all the words within the lexicon to check user ID/password mixtures, or that attack widespread user ID/password mixtures. The attackers will automatism to travel against multiple sites at only once.

3.5 Mistreatment denial of service attacks: The denial of service attack is one among the simplest samples of impacting web site convenience. It involves achieving the server to perform an outsized variety of mundane tasks, prodigious the capability of the server to address the other task.

3.6 Mistreatment server roots exploits: Root exploits consult with techniques that gain super user access to the server. This can be the foremost desired kind of exploit as a result of the chances is limitless. Once you attack a consumer or his computer, you can only have an effect on one individual. With a root exploit, you gain management of the merchants and every one the shoppers' info on the location.

4. Solutions

4.1 Education: Your system is just as secure because the folks that use it. If a client chooses a weak password, or does not stay their password secret, then an attacker will create as that user. This can be important if the compromised password be in the right places to a supervisor of the system.

4.2 Personal firewalls: When connecting your computer to a network, it becomes at risk of attack. A private firewall helps defend your pc by limiting the categories of traffic initiated by and directed to your computer. The interloper also can scan the hard drive to notice any hold on passwords.

4.3 Secure Socket Layer: Secure Socket Layer could be a protocol that encrypts information between the shopper's computer and also the site's server. Once a Secure Socket Layer protected page is requested, the browser identifies the server as a trusty entity and initiates an acknowledgement to pass coding key data back and forth. Now, on resultant requests to the server, the data flowing back and forth is encrypted so a hacker sniffing the network cannot browse the contents.

4.4 Server firewalls: A firewall is just like the trench encompassing a castle. It ensures that requests will only enter the system from such as ports, and in some cases, ensures that every one accesses are only from bound physical machines.

4.5 interruption detection and reviews of security logs: One of the cornerstones of an efficient security strategy is to stop attacks and to observe potential attackers. This helps perceive the character of the system's traffic, or as a place to begin for legal proceeding against the attackers.

4.6 Mistreatment cookies: One of the problems sweet-faced by computing device designers is maintaining a secure session with a consumer over resulting requests. As a result of protocol is homeless, unless some quite session token is passed back and forth on each request, the server has no way to link along requests created by a similar person. Cookies are a preferred mechanism for this. A symbol for the user or session is hold on in an exceedingly cookie and browse on each request. You can use cookies to store user preference data, like language and currency.

5. Conclusion

This paper summarized the solution professionals and security attacks and defenses in an e-Commerce system. Current technology permits for secure website design. It is up to the event team to be each proactive and reactive in handling security threats, and up to the consumer to be open-eyed once searching on-line.

References

[1] 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
[2] Pradnya B. Rane, Dr. B.B.Meshram. "Transaction Security for Ecommerce Application" IJECSE -ISSN- 2277-1956. 2012
[3] Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
[4] Randy C. Marchany, Joseph G. Tront, "E-Commerce Security Issues"Proceedings of the 35th Hawaii International Conference on System Sciences – 2002
[5] 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
[6] Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8 No.5, May 2008

