Volume 4, Issue 3, March 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Network Security Issues in e-Commerce

Raghav Gautam
Student
E&EC Deptt, PEC University of Technology
Chandigarh, India

Sukhwinder Singh
Mentor, Assistant Professor
E&EC Deptt, PEC University of Technology
Chandigarh, India

Abstract— E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security-Integrity, Non-repudiation, Authenticity, Confidentiality, Privacy, Availability. E-Commerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats. Information security, therefore, is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet.

Keywords— Digital E-commerce cycle, E-Commerce , Security Issues, Security measures, Security Threats.

I. INTRODUCTION

E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect e-commerce that include Computer Security, Data security and other wider realms of the Information Security framework. E-commerce security has its own particular nuances and is one of the highest visible security components that affect the end user through their daily payment interaction with business. Today, privacy and security are a major concern for electronic technologies. M-commerce shares security concerns with other technologies in the field. Privacy concerns have been found, revealing a lack of trust in a variety of contexts, including commerce, electronic health records, e-recruitment technology and social networking , and this has directly influenced users. Security is one of the principal and continuing concerns that restrict customers and organizations engaging with ecommerce. Online shopping through shopping websites having certain steps to buy a product with safe and secure. The e-commerce industry is slowly addressing security issues on their internal networks. There are guidelines for securing systems and networks available for the ecommerce systems personnel to read and implement. Educating the consumer on security issues is still in the infancy stage but will prove to be the most critical element of the e-commerce security architecture.

II. PURPOSE OF STUDY

* Study the Overview of E-commerce security.
* Understand the Online Shopping - Steps to place an order.
* Understand the purpose of Security in E-commerce.
* Discuss the different security issues in E-commerce.
* Understand the Secure online shopping guidelines

III. E-COMMERCE SECURITY TOOLS

- Firewalls – For Software and Hardware
- Public Key infrastructure
- Encryption software
- igital certificates
- Digital Signatures
- Biometrics – retinal scan, fingerprints, voice etc
- Passwords
- Locks and bars – network operations centers

IV. PURPOSE OF SECURITY

1. Data Confidentiality – is provided by encryption / decryption.
2. Authentication and Identification – ensuring that someone is who he or she claims to be is implemented with digital signatures.
3. Access Control – governs what resources a user may access on the system. Uses valid IDs and passwords.

4. Data Integrity – ensures info has not been tampered with is implemented by message digest or hashing.
5. Non-repudiation – not to deny a sale or purchase implemented with digital signatures

V. SECURITY ISSUES

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. 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 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.
- Integrity: prevention against unauthorized data
- modification
- Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
- Availability: prevention against data delays or removal.

VI. SECURITY THREATS

- Three types of security threats

–*denial of service,*
–*unauthorized access, and*
–*theft and fraud*

Security (DOS): Denial of Service (DOS)

- Two primary types of DOS attacks: spamming and viruses
- Spamming

–Sending unsolicited commercial emails to individuals
–E-mail bombing caused by a hacker targeting one computer or network, and sending thousands of email messages to it.
–Surfing involves hackers placing software agents onto a third-party system and setting it off to send requests to an intended target.

- DDOS (distributed denial of service attacks) involves hackers placing software agents onto a number of third-party systems and setting them off to simultaneously send requests to an intended target.

•Viruses: self-replicating computer programs designed to perform unwanted events.
•Worms: special viruses that spread using direct Internet connections.
•Trojan Horses: disguised as legitimate software and trick users into running the program

Security (unauthorized access)
•Illegal access to systems, applications or data
•Passive unauthorized access –listening to communications channel for finding secrets.
–May use content for damaging purposes
•Active unauthorized access
–Modifying system or data
–Message stream modification
•Changes intent of messages, e.g., to abort or delay a negotiation on a contract
•Masquerading or spoofing –sending a message that appears to be from someone else.
–Impersonating another user at the ―name‖(changing the From‖field) or IP levels (changing the source and/or destination IP address of packets in the network)
•Sniffers–software that illegally access data traversing across the network.
•Software and operating systems‘ security holes

Security (theft and fraud)
•Data theft already discussed under the unauthorized access section
•Fraud occurs when the stolen data is used or modified.
•Theft of software via illegal copying from company‘s servers.
•Theft of hardware, specifically laptops

VII. SECURE E-COMMERCE GUIDELINES

- *Cookies and History*

Online merchants as well as other sites watch our shopping and surfing habits by using "cookies," an online tracking system that attaches pieces of code to our Internet browsers to track which sites we visit as we search the Web. "Persistent" cookies remain stored on your computer while "session" cookies expire when you turn the browser off.

Online merchants use cookies to recognize you and speed up the shopping process the next time you visit. You may be able to set your browser to disable or refuse cookies but the tradeoff may limit the functions you can perform online, and possibly prevent you from ordering online. Generally, you will need to enable session cookies to place an order. Privacy advocates worry that as more and more data is compiled about us — without our knowledge or active consent — it will be combined to reveal a detailed profile, even our actual identities. This data is often collected to market goods and services to us, encouraging us to buy them. There are a number of companies that specialize in targeted online advertising called "behavioral marketing." Companies say consumers benefit by being exposed to more targeted advertising and that online merchants can make more money more efficiently by targeting the right shoppers.

- Credi*t/ debit card*

The safest way to shop on the Internet is with a *credit card*. In the event something goes wrong, you are protected under the federal Fair Credit Billing Act. You have the right to dispute charges on your credit card, and you can withhold payments during a creditor investigation. The Act also regulates ―negative option‖ plans. A consumer must give express, informed consent before being charged for goods or services sold online through ―negative option‖ marketing, such as ―free trials‖ that the consumer must cancel in order to avoid being charged. Companies that use negative option plans must (1) clearly and conspicuously disclose the material terms of the transaction before obtaining the consumer‘s billing information, (2) obtain a consumer‘s express consent before charging the consumer, and (3) provide a simple mechanism to stop any recurring charges. Online shopping by *check* leaves you vulnerable to bank fraud. And sending a cashier's check or money order doesn't give you any protection if you have problems with the purchase. Never pay for online purchases by using a *money transfer service*.

- *Identity Theft*

As online shopping becomes more common, there will be more cases of identity theft committed over the Internet. Imposters are likely to obtain their victims' identifying information using low-tech means like dumpster diving, mail theft, or workplace access to SSNs. But they are increasingly using the Web to apply for new credit cards and to purchase goods and services in their victims' names. The same advice for avoiding low-tech identity theft applies to shopping on the Internet. Many are mentioned in the above tips. Most important: Be aware of who you are buying from. And use *true* credit cards for purchases, not debit cards. We recommend that you check your credit card bills carefully for several months after purchasing on the Internet. Look for purchases you did not make. If you find some, immediately contact the credit card company and file a dispute claim. Order your credit reports at least once a year and check for accounts that have been opened without your permission.

VIII. CONCLUSION

E-commerce is widely considered the buying and selling of products over the internet, but any transaction that is completed solely through electronic measures can be considered e-commerce. Day by day E-commerce is playing very good role in online retail marketing and peoples using this technology day by day increasing all over the world. E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Dimensions of e-commerce security; Integrity: prevention against unauthorized data modification, No repudiation: prevention against any one party from reneging on an agreement after the fact. Authenticity: authentication of data source. Confidentiality: protection against unauthorized data disclosure. Privacy: provision of data control and disclosure.
Availability: prevention against data delays or removal. Fraudsters are constantly looking to take advantage of online shoppers prone to making novice errors. Common mistakes that leave people vulnerable include shopping on websites that aren't secure, giving out too much personal information, and leaving computers open to viruses. In this paper we discussed E-commerce Security Issues, Security measures, Digital E-commerce cycle/Online Shopping, Security Threats and guidelines for safe and secure online shopping through shopping web sites

REFERENCES

[1] 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
[2] Shazia Yasin, Khalid Haseeb. "Cryptography Based E-Commerce Security: A Review". IJCSI-Vol. 9, Issue 2, No 1, March 2012
[3] Dr. Nada M. A. Al-Slamy, "E-Commerce security" IJCSNS - VOL.8 No.5, May 2008
[4] Seyyed Mohammad Reza Farshchi "Study of Security Issues on Traditional and New Generation of E-commerce Model" International Conference on Software and Computer Applications-IPCSIT vol.9 (2011)
[5] Adams, C., P. Sylvester, M. Zolotarev, and R Zuccherato. 2001. Internet X.509 Public Key Infrastructure data validation and certification server protocols. Internet RFC 3029.
[6] CCITT. 1988. Recommendation X.509: The Directory - Authentication Framework. Data Communications Network Directory, Recommendations X.500-X.521

