International Journal of Computer Engineering Science (IJCES)
Volume 3 Issue 3 (March 2013) ISSN : 2250:3439
https://sites.google.com/site/ijcesjournal http://www.ijces.com/

A Study of Information Security in E- Commerce Applications

Dr. Mohammed Ali Hussain
Professor, Dept. of Electronics and Computer Engineering, KL University, Guntur Dist., A.P., India.

dralihussain@kluniversity.in

Abstract — Electronic Commerce (Ecommerce) refers to the buying and selling of goods and services via electronic channels, primarily the Internet. The applications of E- commerce includes online book store, e- banking, online ticket reservation(railway, airway, movie, etc.,), buying and selling goods, online funds transfer and so on. During E commerce transactions, confidential information is stored in databases as well communicated through network channels. So security is the main concern in E commerce. E commerce applications are vulnerable to various security threats. This results in the loss of consumer confidence. So we need security tools to counter such security threats. This paper presents an overview of security threats to E commerce applications and the technologies to counter them.

Keywords — Authentication, Confidentiality, Integrity, Security, SSL.

I. Introduction

E- Commerce[1] means conducting business online. Selling goods, in the traditional sense, is possible to do electronically because of a certain software programs that run the main functions of an e-commerce Web site, including product display, online ordering, and inventory management. The software resides on a commerce server and works in conjunction with the online payment systems to process payments. Since these servers and data lines make up the backbone of the Internet, in a broad sense, e-commerce means doing business over the interconnected networks. The definition of e-commerce includes business activities that are business-to-consumer (B2C), business-to-business (B2B), extended enterprise computing (also known as "newly emerging value chains"), d-commerce, and m-commerce. Here are a few examples of e-commerce:

- accepting credit cards for commercial online sales
- generating online advertising revenue
- trading stock in an online brokerage account
- driving information through a company via its intranet

- driving manufacturing and distribution through a value chain with partners on an extranet
- selling to consumers on a pay-per-download basis, through a Web site

E-Commerce plays a very important role in the growth of industry as well as convenient and faster method of doing business. As the trend of on-line transactions continues to grow, there will be an increase in the number and types of attacks against the security[2] of on-line payment systems. Such attacks threaten the security of the system, resulting in systems that may be compromised and less protected, resulting in consumer privacy issues. Consumers may be at the risk for losing their personal data, since they may be unaware of the security aspect of performing on-line transactions. Therefore, it is very important to make the Internet safe for buying and selling the products on-line. Global privacy consistency is required, as Internet usage is largely unregulated, which means that the laws in one country are not aligned with the laws in other countries.

This paper presents an overview of security threats to E- commerce applications and the technologies to counter them. This paper is organized as follows: Section 2 presents the need of security in E commerce. Section 3 presents the threats in E commerce applications. Section 4 presents the tools for countering those threats. And finally section 5 presents the conclusion.

II. Need of Security In E-Commerce

The six security needs in E-commerce applications are[3]:

- Access Control.
- Confidentiality.
- Authentication.
- Non Repudiation.
- Integrity.
- Availability.

A. Access Control

Access control ensures only those that authorized require access to resources are given access. This means only the authorized persons are allowed to access the resources.

B. Confidentiality

When information is copied or read by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality or privacy is a very important attribute. Examples include research data, insurance and medical records, new product specifications, and corporate investment strategies. In some locations, there may be a legal obligation to protect the privacy of the individuals. This is particularly true for loan and bank companies; debt collectors;

businesses that extend credit to their customers or issue credit cards; hospitals, doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counselling or drug treatment; and agencies that collect taxes. Information can be corrupted when it is available on an insecure communication network. When information is modified in unexpected ways, the result is known as loss of the integrity. This means that unauthorized changes are made to information, whether by intentional tampering or human error.

C. Authentication

In e-Business, computing and information security it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also very important for authenticity to validate that both parties involved are who they claim they are.

D. Non Repudiation

In law, non-repudiation means one's intention to fulfil their obligations to a contract. It also means that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. E- commerce uses technology such as digital signatures and encryption to establish authenticity and non-repudiation.

E. Integrity

Integrity is particularly important for critical safety and financial information used for activities such as electronic funds transfers, air traffic control, and financial accounting. Information can be erased or become inaccessible, resulting in loss of availability. This means that persons who are authorized to get information cannot get what they need.

F. Availability

For any information system to serve its purpose, the information must be available whenever it is needed. This means that the computing systems used to store and process the information, the security controls used to protect that information, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing the service disruptions due to power outages, hardware failures, and system upgrades.

III. Threats to E-Commerce Security

A.Authentication Attacks

These types of attacks occur when a user changes system resources or gains access to system information without authorization by either sharing logins or passwords or using an unattended terminal with an open session. Password attack is a frequently used method of repeating attempts on a user account and password. They are performed using a program that runs across a network and attempts to log into a shared resource (for example a server).

B. Integrity Attacks

In this type of attack, data or information is added, modified, or removed in transit across the network. This requires root access to the router or a system. If a program does not check the buffer limits when reading or receiving data, this opening can be exploited by an attacker to add arbitrary data into a program or system. When running, this data gives the intruder root access to the system. Integrity attacks can create a delay, causing data to be held or otherwise made unavailable for a period of time. The attackers flood the network with useless traffic, making the system extremely slow to serve the customers, and in the extreme case, causing the system to crash down. They could also cause the data to be discarded before the final delivery. Both delay and denial attacks can result in the denial of service(DOS) to the network users.

C. Confidentiality Attacks

Because network computers communicate serially (even if networks communicate in parallel) and contain limited immediate buffers, data and information are transmitted in small blocks or pieces called packets. The hackers use a variety of methods known collectively as social engineering attacks. With the use of dozens of shareware and freeware packet sniffers available, which do not require the user to understand anything about the underlying protocols, the attackers would capture all network packets and thereby the users login names, passwords, and even accounts. The attackers usually take advantage of human tendency, e.g. using a single, same password for multiple accounts. More often they are successful in gaining access to corporate sensitive and confidential information. Some snooping attacks place the network interface card in promiscuous mode, while the other packet sniffers capture the first 300 bytes of all telnet, file transfer protocol (FTP), and login sessions.

D. Virus

Viruses[4] are computer programs that are written by devious programmers and are designed to replicate themselves and infect specific computers when triggered by a specific event. For example, viruses called macro viruses attach themselves to files that contain macro instructions (routines that can be repeated automatically, such as mail merges) and are then activated every time when the macro runs. The effects of some viruses are relatively benign and cause annoying interruptions such as displaying the comical message when striking a certain letter on the keyboard. Other viruses are more destructive and cause such problems as deleting files from a hard disk or slowing down a system. A network can be infected by a virus only if the virus enters the network through an outside source- for example through an infected floppy disk or a file downloaded from the Internet. When one computer on the network becomes infected then the other computers on the network are highly susceptible to contracting the virus.

E. Trojan Horse

A trojan horse[4] is a malicious code which requires users to invite it in, and is therefore disguised as something else. Unsuspecting users will allow the trojan in to their machine through a seemingly harmless and routine task, only to have their system compromised. A typical trojan horse will be presented as something useful such as an e- mail alert regarding a new security patch. The e- mail might provide a link, inviting the user to click on it to download and install the patch. When the link is followed the trojan gains access to the user's computer and then executes its programmed task. By design, a trojan horse is used by hackers to gain access of a large network or secure system so as to put it to use for its own purposes.

F. Worms

Computer worms[4] are malicious programs designed to spread via computer networks. Computer worms are one form of malware along with the viruses and trojans. A person typically installs worms by inadvertently opening an e- mail attachment or message that contains executable scripts. Once installed on a system, worms spontaneously generate additional email messages contaning copies of the worm. They may also open TCP ports to create networks security holes for other applications, and they may attempt to "flood" the network with spurious Denial of Service (DoS) data transmissions. Being embedded inside everyday network software, computer worms easily penetrate in to most firewalls and other network security measures.

G. Database Threats

E-commerce systems store user personal data and retrieve product information from databases connected to the web-server. Besides product information, databases connected to the web contain valuable and private information that could irreparably damage a company if it were altered or disclosed. Some databases store username and password pairs in a non-secure way. If someone obtains user authentication information, then he/ she can masquerade as a legitimate database user and reveal private and costly information.

IV. Security Technologies

Two types of encryption methods offer reliable protection to E- commerce businesses. They are symmetric and asymmetric.

A.Symmetric Encryption

Symmetric encryption[4][5] may also be referred to as single key or shared secret encryption. In symmetric encryption, a single key is used both to encrypt and decrypt messages. Common symmetric encryption algorithms include AES, DES, 3DES, and RC4. Symmetric encryption algorithms can be extremely fast, and low complex which allows for easy implementation in hardware. However, they require that all hosts participating in the encryption have already been configured with the shared secret key through some external means.

B.Asymmetric Encryption

Asymmetric encryption[4][5] is also known as public-key cryptography or two-key encryption. Asymmetric encryption differs from symmetric encryption primarily in that two keys are used: one for encryption and other for decryption. The most common public key encryption algorithm is RSA. Compared to shared key encryption, asymmetric encryption imposes a high computational burden, and tends to be much slower. its major strength is its ability to establish a secure channel over a non- secure medium (for example, the Internet). This is accomplished by the exchange of public keys, which can only be used to encrypt information. The complementary private key(non shared) is used to decrypt.

C.Secure Socket Layer

The E-commerce business is all about making money and finding ways to make more and more money. But that's hard to if the consumers don't feel safe executing a transaction on your Web site. Secure Socket Layer(SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. When you have SSL, you are protected as well as your customer. The server – which is basically another name for a computer that stores information about your website for viewing by the customers and others – must have a digital SSL certificate. SSL provides these certificates and is able to read them. SSL certificates come from a trusted third party that can guarantee encryption process. The SSL certificate is a proof that the server is what it says it is. Having a SSL makes it harder for fraudsters to pretend to be another server.

D. Digital Signature

Based on the public-key cryptographic method combined with data hashing functions such as MD-5 and SHA-1, digital signatures are implemented to verify the origin and contents of the online transaction, translating to consumers proving their identity to vendors in the transaction and providing non-repudiation features.

A digital signature[8] functions for an electronic document like a handwritten signature does for printed documents. The hand written signature is an unforgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached. A digital signature actually provides a greater degree of security than the handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been modified either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated, this means the signer of a document cannot later disown it by claiming the signature was forged. In other words, digital signatures enable "authentication" of digital messages, assuring that the recipient of a digital message of both the identity of the sender and the integrity of the message.

E. Digital Certificates

Digital Certificates provide a means of proving a persons identity in electronic transactions, much like a driver license or a passport does in face-to-face interactions. With a Digital Certificate, you can assure business associates, friends and online services that the electronic information they receive from you are authentic. Digital Certificates bind an identity to a pair of electronic keys that can be used to encrypt and sign the digital information. A Digital Certificate makes it possible to verify someone's claim that they have the right to use a given key, helping to prevent users from using phony keys to impersonate other users. A Digital Certificate is issued by a Certification Authority (CA) and signed using the CA's private key. Digital Certificates can be used for a variety of electronic transactions which includes e-mail, electronic commerce, groupware and electronic funds transfers.

F. Smart Cards

A smart card[6] can generally be defined as a plastic card with dimensions similar to traditional debit/credit cards, into which an electronic device has been incorporated to allow information storage. Frequently, it also has an integrated circuit chip with data processing capacity. Smart cards are normally separated into two categories: microprocessor cards and memory cards, commonly named smart cards for their capability to do data processing and the sophisticated algorithms embedded in them. The lack of security and a fear of hackers are some of the reasons that have caused the slow growth of the online interactive commercial transactions among individuals and enterprises, generally called consumer–to-business (C2B) e-commerce. In spite of the number of these breaches, credit cards are being used as one of the payment mechanisms over the Internet. As long as commercial transactions over the Internet are not too great in the number and have a small individual economic value, the actual threat could be considered at a low or acceptable risk level. Once this type of transaction gains more consumer confidence and the volume increases, it will attract more and more fraud activities, thus increasing the level of risk exposure. One of the techniques that has begun to be used in France and other countries is the smart card with a C-SET(Chip-Secure Electronic Transaction) protocol for online authentication. This authenticates both the card as well as the customer, and therefore offers a payment guarantee without customer non-repudiation.

G. Electronic Money

Electronic money or digital cash (DC)[7] is an electronic method of payment on the Internet with the result that money is transferred from one account to another. One can visualize a DC transaction as a foreign exchange market, in the sense that money is converted to DC before it can be spent. When making a purchase, a buyer will send a 'digital coin' message encrypted with its private key containing his identity, the amount of the coin, Internet address, its serial number and expiry date. A record is kept of that transaction to ensure that the coin is not double spent. The digital coin is also encrypted with the merchant's public key. The merchant decrypts the digital coin with his private key and verifies the message. The issuer must verify the serial number of the digital coin to confirm that it is still current and has not been already spent. The issuer then credits the merchant's bank account with the currency and then cancels the serial number.

V. Conclusion

Security in electronic commerce is becoming more topical as the shift from traditional shopping and transactions move away from physical stores to online. Security has three main concepts- confidentiality, integrity, and availability. Confidentiality ensures that only authorized parties to read protected information. Integrity ensures that data remains as is from the sender to the receiver. Availability ensures that you have access and are authorized to resources. Globally E-commerce is growing but however it comes with a risk that some part of the transaction is compromised which may lead to financial loss or unindented shared private information. It is therefore the security of e-commerce transactions that is a critical part of the ongoing success as well as growth of E-commerce. The security threat of E commerce includes viruses, worms, Trojan horse, Denial of service, password thefting. The technologies for protecting E commerce transactions include encryption of data, SSL, digital signature, digital certificates, smart card, e- cash.

References

[1] L. X. QIN Zhiguang, GAO Rong, "A survey of E-commerce Security," Electronic Science and Technology of China vol. 2, no. 3, Sept 2004.

[2] Xu Wei, “e-commerce online payment security issues”. joint Hefei University Journal, 2000 (3), pp:23-25.

[3] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24- 28, Sep 1998.

[4] William Stallings, “Cryptography and Network Security”, 3rd edition, Prentice Hall,2003.

[5] Schneier, B. 1996. Applied Cryptography. New York: John Wiley & Sons.

[6] Rankl, W., and W. Effing. 1997. The Smartcard Handbook. New York: John Wiley.

[7] Brands, Stefan. 1996. Electronic Cash. Invited talk, RSA Cryptographers' Colloquium.

[8] L Lamport, “ Constructing digital signatures from a one way function “ SRI Intl, CSL, 1998.

AUTHOR PROFILE

Dr. Md. Ali Hussain M.Tech., Ph.D. working as Professor Dept. of Electronics and Computer Engineering, KL University, Guntur District, A.P., India. His research interest includes Computer Networks, Wireless Networks, Mobile Networks and Web Commerce. He has published large number of papers in National & International Conferences and International Journals. He also served as a Program Committee (PC) Member for many International Conferences. He is at present Chief Technical Advisory Board Member, Chief Editor, Editor and Technical Reviewer of reputated International Journals. **Received Best Academic Researcher Award 2012 from ASDF Research Group, Supported by Government of Pondicherry.** He is a member of IACSIT, IRACST, UACEE, ISTE, IAENG, AIRCC, AICIT, and IARCS.