

Security Issues in E-Commerce

Diana J. Fernandes

Assistant Professor, Department of Computer Science, B. K. Birla College of Arts, Science and Commerce, Kalyan

Abstract

Nowadays, various companies and organizations are utilizing the web in order to acquaint people with their products or services all around the globe. E-commerce (electronic commerce) or EC is about selling and buying of goods and services which is basically the exchange of goods and services, over the internet. E-commerce can be any type of commercial or business transaction that involves the transfer of data or funds across the internet. One of the foremost issues in every electronic commercial process is Security which is a part of the Information Security framework. It affects e-commerce as well as Data Security, Computer security and so on. Thus, weakening customer's confidence in e-commerce and e-business.

This paper highlights e-commerce security issues and postulates some techniques for preventing from security threats and vulnerabilities.

Keywords: E-commerce, security issues, vulnerability, threats, cyber security

Introduction

In today's modern business, E-commerce is flourishing across the globe. E-commerce delivers numerous benefits to the consumers in form of availability of goods and services in wider choice and at lower cost which saves a lot of time. E-commerce is more than just enhancing the existing business practices. Ecommerce can be divided into two parts: E-finance & E-Merchandise. By the mid of 2020, India is expected to generate \$100 billion online retail revenue and it is likely to grow four times in the coming years. It is a 'disruptive' innovation that is drastically changing the traditional way of doing business. The site uses digital shopping basket system or digital shopping cart and allows e-payment through debit card, credit card, or EFT (Electronic fund transfer) payments.

The advent of electronic transaction using mobiles has become very popular and is in great demand among people. One of the major reasons is that people can use electronic transaction while making payments easier at their convenience. Hence, Security for electronic transaction is obligatory because its confidential information such as credit card numbers, debit card numbers, pin numbers and other information for which security is needed.

Some of the security issues in electronic transaction application are listed below:

- **Malicious code** – It is a code which intend to cause damage to a system, undesired effects or security breaches. Major malicious code are as follows:
 - Viruses: The viruses have capability to replicate and spreads to other files which includes file infecting viruses, macro viruses, and script viruses.
 - Worms: They are alike to viruses but it is intended to spread from computer to computer.
 - Trojan horse: They give illegitimate user control over the infected computer.
- **Denial of Service (DOS) Attack** - In a denial of service (DoS) attack, hackers flood the Web server or network server with thousands of false requests for services to crash the network. Because of which the legitimate users are not able to access resources and services.
- **Spoofing and Sniffing** - Hackers attempts to hide their true identities often misrepresent or spoof, themselves by using fake e-mail addresses or masked as someone else. Which simply means that the attacker attempts to gain unauthorized access to computer data by pretending to be an authorized user. It may also involve redirecting a Web link to an address (fake site) different from the intended one. A

sniffer is an eavesdropping program which monitors information travelling over the internet. For instance, when transaction information is transmitted through the Internet, hackers can intercept the transmission and acquire customers' confidential information like debit card number, credit card number, username, password, pin number, etc. The content of a transaction may not only be intercepted, but can also be altered maliciously.

- **Hacking** - It's an attempt to access others computer data without the person knowing about it.
- **Credit card fraud** - In this illegitimate user uses others credit card pin for its personal use.
- **Overcharge** - The fraudulent activities contain charging the customers higher price than the agreed prices for the good or service.

E-Commerce Security Tools

Some of the tools which can be implemented for E-Commerce security is listed below:

- **Firewalls** – Firewalls are basically software or hardware security measure that filters the information passing between an internal and external network. A firewall controls access to network by internal users, and also thwarts outsiders from access to the systems and information stowed on the internal network. A firewall can be in any one forms: Network firewall or Software firewall.

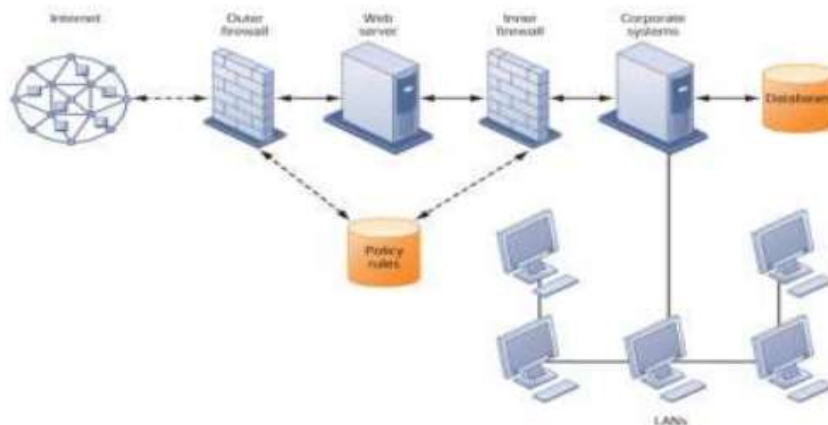


Figure 1: Implementation of Firewall

- **Public Key infrastructure** - A public key infrastructure (PKI) is a set of policies, roles, software, hardware, and software required to create, store, distribute, manage, distribute, use and revoke digital certificates and manage public-key encryption. PKI is implemented to facilitate secure electronic transfer of information over the internet.



Figure 2: Public Key Infrastructure (PKI)

- **Digital certificates** - Digital certificates are data files which is used to establish the identity of users and electronic assets for protection of online transactions. Digital certificate system uses certificate authority (CA), a trusted third party to validate a user's identity. The CA verifies a digital certificate user's identity and this information is stored on the CA server, which generates an encrypted digital certificate containing a copy of the owner's public key and owner's identification information. The certificate authenticates that the public key belongs to the designated owner. The CA makes its public key available publicly. The recipient of an encrypted message uses CA's public key to decode the digital certificate attached to the message and is verified. It thus obtains the sender's public key and identification information contained in the certificate. Using this data, the recipient can send an encrypted reply. The digital certificate system would enable to validate that a trusted third party and authorized party issued their digital certificates before they exchange data, for example, credit card user, merchant, etc.
- **Digital Signatures** - In E-commerce system, digital signatures are adopted to sign authorizations (license) between participating users for transmitting digital content over the internet. Thereafter, this license is used as a proof of usage rights. At the client side, license is confirmed for the verification of the usage rights.

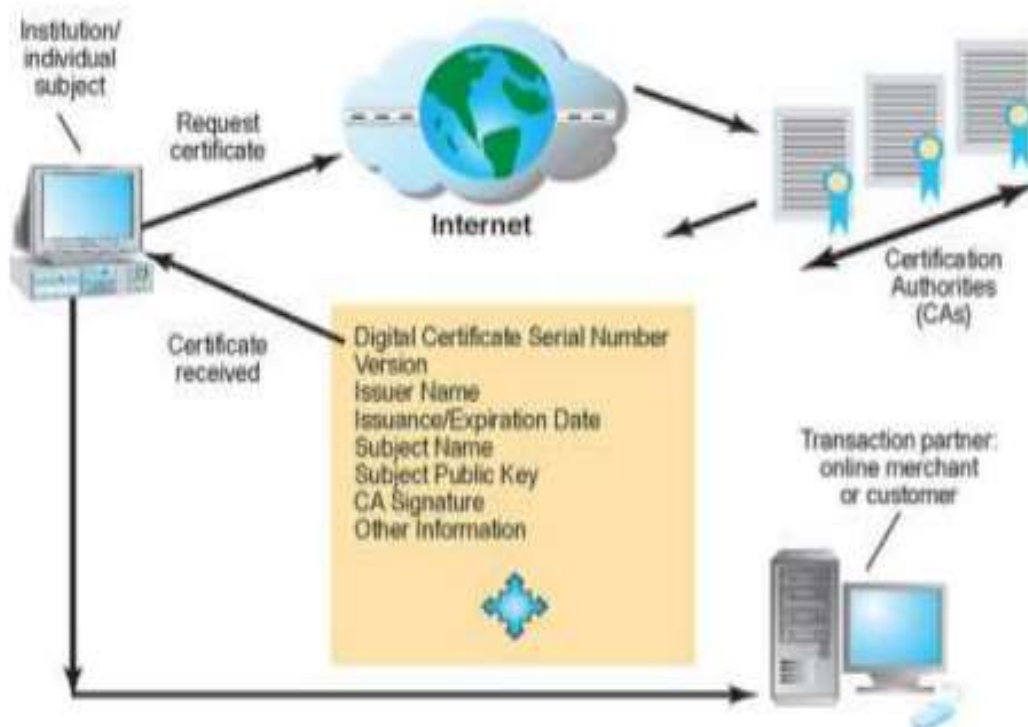


Figure 3: Digital Certificate and Digital Signature

- **Biometrics** - Biometric authentication is based on the measurement of behavioural or physical trait that makes each individual unique. Biometric authentication uses systems that read, interpret, compares an individual's unique characteristics, such as the face, fingerprints, or retinal image, against a stored profile in order to grant or deny access
- **Secure Socket Layer (SSL)** - SSL is a security protocol developed by Netscape Communications that works to protect the communication by server authentication, encryption over the Internet.
- **Secure Electronic Transaction (SET)** - SET protocol is designed to ensure the integrity and security of online purchases and communications. Secure Electronic Transaction protocol uses digital certificates to perform a series of security by verifying the identity of a customer or sender of information. Digital signatures, digital certificates and digital wallets operate according to the SET protocol.

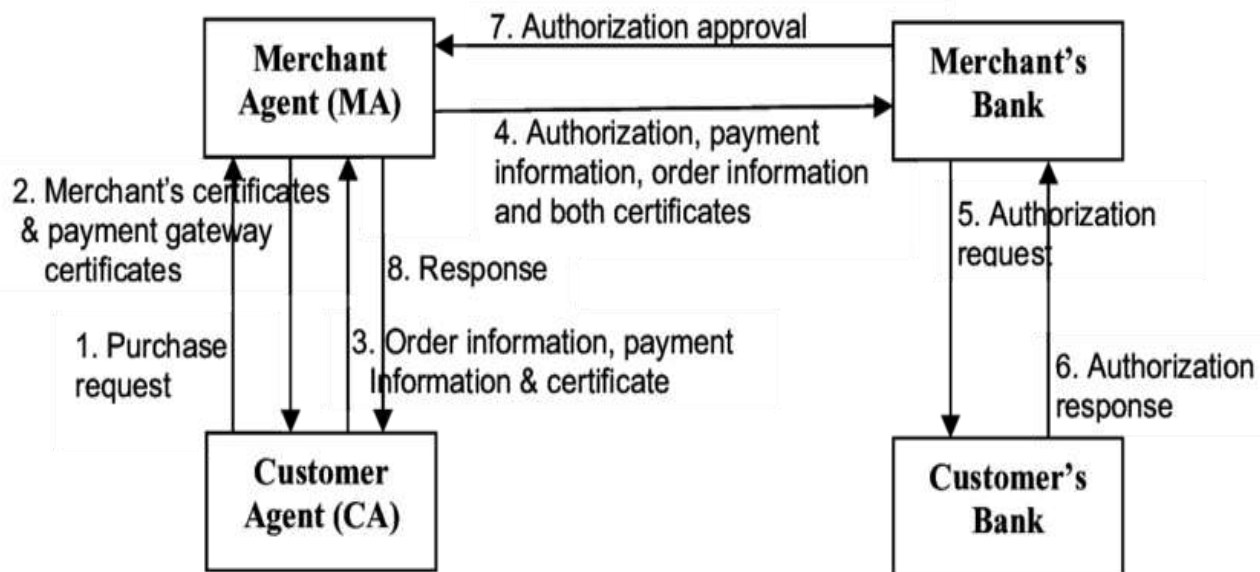


Figure 4: Secure Electronic Transaction (SET)

GUIDELINES FOR SECURITY

Some precautions which can be followed for secure transaction are as follows:

- Security Software - Install the security software in your computers so that it can protect the sensitive data.
- Use encryption signs for the password - When you do a login, make sure that the password will get encrypted. When it is transmitted over the network it will not be used by anyone.
- Different password - Use different password for different accounts and keep changing your passwords periodically so it cannot be misused by anyone else if another person knows your password.
- Dealing with offers - While purchasing products from E-Commerce site, be sure about the site and the product. While using promotional offers, it is desirable to go directly to the seller site.
- Avoid public computers - For financial transaction never use any public computers instead always use the personal computer.
- Avoid public Wi-Fi - Financial Transactions over a public Wi-Fi connection is highly unsafe. There are possibilities of your data to be hacked by hacker. Also, make sure that you connect to the internet using a secured Wi-Fi connection which is password protected.
- Purchase product from reputed sites - Always buy products from reputed site to make sure that your security is not compromised. Also check the confirmation Email once you complete e-payment.
- Data Encryption - Confidential or sensitive customer data like debit card number, credit card number, pin number is encrypted by using cryptographic algorithms to protect data transmission over internet.
- Adopt Access Control List (ACL) - ACL restricts different groups of unauthorized users to access information and confirms that only the intended users have access to data and services.

CONCLUSION

With the increasing dependence on e-commerce, it is certain that the total volume of transaction will only increase in the near future. Lack of appropriate security protocols puts the online store owner, e-commerce, websites, reputation and eventually the end consumer at a risk. And this risk includes both financial consequences and compromise data privacy. Enforcing and updating the existing security measures already in place will go a long way in preventing payment fraud and data breach.

REFERENCES

1. Alka Raghunath, 2013. "Problem and Prospects of ECommerce ", International Journal of Research and Development - A Management Review (IJRDMR) ISSN (Print): 2319-5479, Volume-2, Issue – 1, 2013 68
2. Abhijit Mitra 2013. "E-commerce in India- a review", International Journal of Marketing, Financial Services and Management Research ISSN 2277- 3622 Vol.2, No. 2, February (2013)
3. Chanana Nisha and Goele Sangeeta, "Future of e-commerce in India", International Journal of Computing & Business Research, ISSN (Online): 2229-6166
4. Stuart Feldman, "The Changing Face of E-Commerce: Extending the Boundaries of the Possible", IEEE INTERNET COMPUTING, MAY -JUNE 2000, pp:82-83
5. DonalO.Mahony, Michael Peirce Hitesh Tewari, "Electronic Payment Systems for E-Commerce ", Artech House computer security series-Boston 2001, Second Edition, pp: 19-69
6. Smith.R and Shao.J, "Privacy and e-commerce: a consumer-centric perspective", Electronic commerce research, vol. 7, no. 2, (2007).
7. Randy C. Marchany, Joseph G. Tront (2002). E-Commerce Security. Issues "Proceedings of
8. the 35th Hawaii International Conference on System Sciences – 2002