Research Paper Management

Cyber Security; Issue and Challenges in E-Commerce

Santosh Kumar Maurya UGC- NET/JRF Research Scholar, Department of Management Studies, Nehru Gram Bharati University, Allahabad

NagendraPratap Bharati UGC- RGNSRF Research Scholar, Department of Management Studies, Nehru Gram Bharati University, Allahabad

ABSTRACT

E-Commerce refers to the exchange of goods and services over the Internet. The shopping through e-commerce has penetrated all segments of goods ranging from groceries to electronic goods and even vehicles. Rapid growth in mobile computing and communication technologies has facilitated popularity of e-commerce. The main impediment in growth of e-commerce is cyberfraud and identity theft. Hackers are people who carry out the cybercrime. Hence, poor security on e-Commerce web servers and in users computers is core issue to be resolved for rapid growth of e-commerce. This paper provides directions for e-commerce security so as to improve customer confidence in e-commerce shopping.

KEYWORDS e-Commerce, Security, Threats and Vulnerabilities, Firewall, Session Hijack, Viruses.

Introduction

The rapid evolution of online and mobile channels has carved out new markets and brought huge opportunities for emergent and established organizations alike. However, unfortunately the past decade has also witnessed significant disruption to ecommerce payment processes and systems. The interconnected, anonymous and instantaneous nature of these channels has inevitably led to the development of malicious threats targeting ecommerce and retail services firms, their people and their customers. These e-crime and digital fraud threats continue to evolve rapidly, with attackers utilizing increasingly sophisticated techniques to target vulnerabilities in people, processes and technologies. The e-crime threats, if successfully realized, can undermine essential digital services, cause significant damage to brand reputations, and result in considerable financial and operational pain for organizations and their customers.

In order to achieve the security objectives, it is necessary to recognize that the security of the services and the protection of the customers' data are essential. To this end, and specifically to support the current security equation, it is necessary to have an enterprise wide target customer security model. This should be designed to deliver enhancements to both customer-facing and back office security capabilities, and in particular to improve existing security defenses for remote online, telephone and mobile banking channels.

RELATED WORKS

Security is one of the principal and continuing concerns that restrict customers and organizations engaging withecommerce. The aim of this paper is to explore the perception of security in e-commerce B2C and C2C websites from both customer and organizational perspectives.

With the rapid development of E-commerce, security issues are arising from people's attention. The security of the transaction is the core and key issues of the development of E-commerce. This paper about the security issues of E-commerce activities put forward solution strategy from two aspects that are technology and system, so as to improve the environment for the development of E-commerce and promote the further development of E-commerce.

Web applications increasingly integrate third-party services. The integration introduces new security challenges due to the complexity for an application to coordinate its internal states with those of the component services and the web client across the Internet.

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. Still, its definition is a complex endeavor due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions.

Objective of Study

- Study the Overview of E-commerce security.
- Understand the purpose of Security in E-commerce.
- Third Party risk in Online Shopping.

E-COMMERCE SECURITY TOOLS

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

Security issues in e-commerce application

There are following types of security issues in any e-commerce application which needs to be addressed

Malicious Code:

- Viruses: They have ability to replicate and spread to other files; most also deliver a "payload" of some sort (destructive or benign); include macro viruses, file-infecting viruses, and script viruses
- Worms: They are designed to spread from computer to computer
- Trojan horse: They appears to be benign, but then does something other than expected
- Bots: It can be covertly installed on computer; responds to external commands sent by the attacker

Unwanted Programs: These are installed without the user's informed consent. Following are its types. Browser parasites: It can monitor and change settings of a user's browser Adware: It calls for unwanted pop-up ads

Spyware: It can be used to obtain information, such as a user's keystrokes, e-mail, IMs, etc.

Phishing and Identity Theft: Any deceptive, online attempt by a third party to obtain confidential information for financial gain – Most popular type: e-mail scam letter – It is one of fastest growing forms of e-commerce crime.

Hacking and Cyber vandalism: Hacker: Individual who intends to gain unauthorized access to computer systems

- Cracker: Hacker with criminal intent (two terms often used interchangeably)
- Cyber vandalism: Intentionally disrupting, defacing or destroying a Web site.

Transaction Security for E-commerce Application

1. Encryption Approach

Encryption is the process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and the receiver. The purpose of encryption is:

(a) To secure stored information and
(b) To secure information transmission.

There are several types of encryption that differs in the context of its functionalities.

2. Secure Socket Layer

The most common form of securing channels is through the Secure Sockets Layer (SSL) of TCP/IP. The SSL protocol provides data encryption, server authentication, optional client authentication, and message integrity for TCP/IP connections. Secure Socket Layer (SSL) is a security protocol, first developed by Netscape Communications Corporation and now taken over by the transport layer security working groups. The design goal of the protocol is to prevent eavesdropping, tampering or message forgery when a data is transported over the Internet between two communicating applications.

3. Secure Hypertext Transfer Protocol (S-HTTP)

S-HTTP is a secure message-oriented communications protocol designed for use in conjunction with HTTP. It is designed to coexist with HTTP and to be easily integrated with HTTP applications. Whereas SSL is designed to establish a secure connection between two computers, S-HTTP is designed to send individual messages securely. Using S-HTTP, any message may be signed, authenticated, encrypted or any combination of these. Generally, S-HTTP attempts to make HTTP more secure.

4. Digital Signature

Digital signature means a digital method executed by a party with the intent to authenticate a record, which is a unique to the person using it and is capable of verification. It is linked to the data in such a manner that if the data is changed, the electronic signature is invalidated. A digital signature is normally a hash of the message which is encrypted with the owner's private key.

5. Secure Electronic Transaction (SET)

A SET specification for credit/payment card transactions is required for the safety of all involved in e-commerce. It is designed to meet three main objectives. First, it will enable payment security for all involved, authenticate card holders and merchants, provide confidentiality for payment data and define protocols and potential electronic security service providers. It will also enable interoperability among applications developed by various vendors and among different operating systems and platform.

6. Digital Certificate

A digital certificate is a digital document issued by a trusted third party institution known as a certification authority that contains the name of the subject or company, the subject's public key, a digital certificate serial number, an expiration date, an issuance date, the digital signature of the certification authority and other identifying information. The Certification Authority (CA) is a trusted third party that hands out certificates and publishes identities and public keys in a directory. The certificate is signed with the private key of the Certification Authority; therefore, its authenticity can be confirmed by using the known public key of the CA.

Recommendations

The rapid pace at which technology is changing has provided large opportunities for organizations to develop new business models, services, and products. While the digital revolution has transformed the way we do business, it has also created complex and sophisticated security issues. Assets and Information that were once protected within the organization are now accessible online; customer channels are vulnerable to disruption; criminals have new opportunities for theft and fraud. With organizations growing organically and inorganically, complexity of managing businesses & security operations are also becoming complex.

Organizations today thus face a continuously evolving threat landscape where the speed and intensity ofattack is incrementing and response time is subsiding. As a result, organizations need to have rapid detectionand response capabilities that allow for the synthesis of external and internal threat intelligence in a timely manner. This "situational awareness" is a required component of an organization's overall security posture and critical to maintaining the confidentiality, integrity, and availability of its information assets. Some of the key recommendations for an organization to step towards an effective security equation include:

- Set risk appetite and drive focus on what matters. Establish purpose and direction. Clearly articulate your cyber risk appetite and strategy. Support it by requisite action through funding and resourcing.
- Define the right balance between threat-centric vs. compliance-centric programs. Fully integrate cyber risk management into IT disciplines.
- Break down silos. Cyber risk is an enterprise-level issue. Lack of information-sharing is a top inhibitor for effective risk management.
- Be creative about cyber risk awareness. Your weakest link is the human factor. There is not enough talent to do everything in-house, so take a strategic approach to sourcing decisions.
- Incentivize openness and collaboration. Build strong relationships with partners, law enforce -ment, regulators, and vendors.
- Prepare for cyber-attacks by conducting war games, penetration tests, and exercising the cyber incident response plans.
- Have a threat intelligence mechanism in place Focus on restructuring the diverse unstructured security data and information gathered from all the security entities and devices (recent and past events) to consolidate intelligent feeds, advice or a product, which could be used to make informed decisions in order to mitigate dynamic threats as pet the environment.

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 and M-commerce 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 datadisclosure. Privacy: provision of data control and disclosure.

REFERENCES

1. Review of e-Commerce Security Challenges by Jarnail Singh in International Journal of Innovative Research in Computer and Communication Engineering. | 2. Stuart Feldman, “The Changing Face of E-Commerce: Extending the Boundaries of the Possible”, IEEE INTERNET COMPUTING, MAY -JUNE 2000, pp:82-83 | 3. JOSE A. ONIEVA, “Multiparty Nonrepudiation: A Survey”, ACM Computing Surveys, Vol. 41, No. 1, Article 5, December 2008, pp:5.1-5.42 | 4. Adam Jolly, “The Secure Online Business”, Great Britain and the United States- Kogan Page Limited 2003, pp: 93-118 | 5. PETER C. CHAPIN, CHRISTIAN SKALKA, and X. SEAN WANG, “Authorization in Trust Management: Features and Foundations”, ACM Computing Surveys, Vol. 40, No. 3, Article 9,August 2008,pp: 9.1-9.48 | 6. DonalO.Mahony, Michael Peirce Hitesh Tewari, “Electronic Payment Systems for E-Commerce“, Artech House computer security series-Boston 2001, Second Edition, pp: 19-69 | 7. MohitKabra Chief Financial Officer, MakeMyTrip.in Future of e-Commerce: Uncovering Innovation page no.27 |