E-COMMERCE SYSTEM: A REVIEW ON SECURITY CHALLENGES AND INDIAN PERSPECTIVE

[1] MR. HARDIK NARIYA, [2] PROF. CHIRAG GOHEL

[1]M.E.[Computer Engineering] Student, Department Of Computer Engineering, Marwadi Education Foundation Group of Institutions, Rajkot, Gujarat
[2] Asst. Professor, Department Of Information Technology, Marwadi Education Foundation Group of Institutions, Rajkot, Gujarat

hardik.b.nariya@gmail.com

ABSTRACT: *As the network technologies and Internet users are growing more and more, online business has become popular. So, now a day E-Commerce system is being used by large no. of peoples Lowering the cost of operation, increase the speed of transactions and easy global reach to customers and vendors have been the reasons for the overwhelming popularity of this new way of Commerce. There are many security concerns involved in E-Commerce system in which there are many sensitive data are transferred across communication channel. This concerns range from the verification for the identities of people concerned to the protection and validity of data in transfer. In this paper will discuss E-Commerce system and Security concerns of different part for improving reliance of E-Commerce for business transactions and various ways by applying different techniques to minimize these threats.*

Keywords— E-Commerce, security.

I: INTRODUCTION

E-Commerce offers lower transactions cost, more timely execution and improved market efficiency. Benefit includes increased trade, a wealthier society and a more equitable distribution. However lack of assurance about security is the greatest barrier currently affecting the growth of E-Commerce. Consumers must have confidence that their electronic transactions will remain private and unaltered. Consumers must trust the system to prevent fraud and keep their transactions private. Businesses require assurance that their systems and digital assets will remain safe from security intrusions, sabotage, and fraud. For E-Commerce to reach its potential confidence in the security of the system must be assured (Greenstein, 1999).

What is E-Commerce?

E-Commerce refers to the exchange of goods and services over the Internet. All major retail brands have an online presence, and many brands have no associated bricks and mortar presence. However, E-Commerce also applies to business to business transactions, for example, between manufacturers and suppliers or distributors. In the online retail space, there are a number of models that retailers can adopt. Traditionally, the Web presence has been kept distinct from the bricks and mortar presence, so transactions were limited to buying online and delivering the goods or services.

The online presence is also important for researching a product that a customer can purchase later in the store. Recently, there has been a trend towards multi-channel retail, allowing new models such as purchasing online and picking up in store.

E-Commerce systems are also relevant for the services industry. For example, online banking and brokerage services allow customers to retrieve bank statements online, transfer funds, pay credit card bills, apply for and receive approval for a new mortgage, buy and sell securities, and get financial guidance and information.

Security research

Security measures involve interaction of users, hardware, and software. A good security system should not only look at hardware and software, it should also cover other areas such as physical security, human security, business and disaster protection, and legal implications. Because of the diverse nature of E-Commerce, we need to address all these security issues. For example, we can provide good network security but it might depend on the particular country's encryption rules. Even if every other aspect is catered for, there still might be a security risk if a particular business is located in the war-zone. Hence, we have to consider all these areas in order to find solutions for E-Commerce security. This research investigates the major factors that influence the type of external Security measures required and implemented by an organization. Factors include: technical, reputation, societal, legal, and management factors.

Why is this research important?

Prior to this research there are some work, which has been completed in this area. The security measurement on most of these previous studies is depending upon computer systems and data contained within them. The main focus of this research is to identify the factors that are influential to the measurements of security. They are broken down into several groups according to the aspect of protection being address, from minimal to specific. The model used in this research will be able to identify security measurements, specific to the business requirements, or improve an existing program. The security system described in this research can be used to avoid overall technical and non-technical security problems in the organization and how to manage the design process and the resulting security program. This model will help organization to reduce security concerns, ensure business continuity and avoid minimize business damage, protect organization.

II: TECHNICAL COMPONENTS OF E-COMMERCE SECURITY

There are four components involved in E-Commerce Security: client software, server software, the server operating system, and the network transport. Each component has its own set of issues and challenges associated with securing them:

- Client software is becoming increasingly more security-focused; however single-user desktop operating systems historically have had no security features implemented. E-Commerce software that relies on the security of the desktop operating system is easily compromised without the enforcement of strict physical controls.

- Server software is constantly under test and attack by the user community. Although there have been cases of insecurities, a system administrator keeping up with the latest patches and vendor information can provide a high degree of confidence in the security of the server itself.

- Operating systems used for hosting E-Commerce servers are securable, but rarely shipped from the vendor in a default configuration that is secure. E-Commerce servers must protect the database of customer information accumulating on the server as well as provide security while the server is handling a transaction. If it is easier for a thief to compromise the server to obtain credit card numbers, why bother sniffing the network for individual credit card numbers?

- Session transport between the client and server uses network protocols that may have little or no built-in security. In addition, networking protocols such as TCP/IP were not designed to have confidentiality or authentication capabilities.

Why No Unified Standard Method

The methods and models of securing E-Commerce transactions are as diverse as the transactions themselves. E-Commerce transactions are performed with varying levels of security, from sending requests in the clear, to encrypted password protection, to using digital certificates.

So why not simplify things by implementing one standard method for securing E-Commerce transactions? The problem with creating one standard solution is that there are different and sometimes conflicting goals in securing a transaction. The objectives of the merchant may not be the same as those of the user or bank. The merchant, for example, requires a valid transaction, liability coverage, and payment for goods and services. The user would like to purchase a product, protect privacy (name, address, and payment information), and pay for only the products they have agreed to purchase. The institutions providing payment would like to detect and prevent fraud. Many security solutions address one or more of these security goals—but where one solution may focus on providing privacy, another may focus only on transaction validation.

In addition to the differences in security goals, vendors and governments introduce complications into selecting security standards for E-Commerce. Vendors disagree on implementations and try to push their own products into standards. National governments try to limit and control use of encryption to secure E-Commerce transactions. One of the benefits of E-Commerce is that it allows a small company to distribute and sell products globally. But national laws and regulations can dilute the standards to the lowest common denominator.

E-commerce security system can be divided into two categories E-commerce transaction security and network security. E-commerce transaction security focuses on problems occurring when the traditional business is operated on the internet. It secures all the E-transactions to be processed safely by using network security as a base.

Fig 1: Architecture of EC Security Technology

The E-Commerce security architecture is made up of five parts shown in figure. 1. Each layer builds its functionality on the layer beneath it and provides technical support to its upper layer. Computer network security can be divided into Physical layer, Data Link Layer, Network Transmission Layer, Commerce Transaction Layer and Application system layer.

III: TYPES OF ATTACKS IN E-COMMERCE SYSTEM

- Eavesdropping
- Snooping
- Interception
- Modification Attacks
- Repudiation Attacks
- Denial-of-service (DoS) Attacks
- Distributed denial-of-service (DDoS) Attacks
- Back door Attacks
- Spoofing Attacks
- Man-in-the-Middle Attacks
- Replay Attacks
- Password Guessing Attacks

Eavesdropping - This is the process of listening in or overhearing parts of a conversation. It also includes attackers listening in on your network traffic. It's generally a passive attack, for example, a co-worker may overhear your dinner plans because your speaker phone is set too loud. The opportunity to overhear a conversation is coupled with the carelessness of the parties in the conversation.

Snooping - This is when someone looks through your files in the hopes of finding something interesting whether it is electronic or on paper. In the case of physical snooping people might inspect your dumpster, recycling bins, or even your file cabinets; they can look under your keyboard for post-It-notes, or look for scraps of paper tracked to your bulletin board. Computer snooping on the other hand involves someone searching through your electronic files trying to find something interesting.

Interception - This can be either an active or passive process. In a networked environment, a passive interception might involve someone who routinely monitors network traffic. Active interception might include putting a computer system between sender and receiver to capture information as it is sent. From the perspective of interception, this process is covert. The last thing a person on an intercept mission wants is to be discovered. Intercept missions can occur for years without the knowledge of the intercept parties.

Modification Attacks - This involves the deletion, insertion, or alteration of information in an unauthorized manner that is intended to appear genuine to the user. These attacks can be very hard to detect. The motivation of this type of attack may be to plant information, change grades in a class, alter credit card records, or something similar. Website defacements are a common form of modification attacks.

Repudiation Attacks - This makes data or information to appear to be invalid or misleading (Which can even be worse). For example, someone might access your email server and inflammatory information to others under the guise of one of your top managers. This information might prove embarrassing to your company and possibly do irreparable harm. This type of attack is fairly easy to accomplish because most email systems don't check outbound email for validity. Repudiation attacks like modification attacks usually begin as access attacks.

Denial-of-service Attacks - They prevent access to resources by users by users authorized to use those resources. An attacker may try to bring down an E-Commerce website to prevent or deny usage by legitimate customers. DoS attacks are common on the internet, where they have hit large companies such as Amazon, Microsoft, and AT&T. These attacks are often widely publicized in the media. Several types of attacks can occur in this category. These attacks can deny access to information, applications, systems, or communications. A DoS attack on a system crashes the operation system (a simple reboot may restore the

server to normal operation). A common DoS attack is to open as many TCP sessions as possible; this type of attack is called TCP SYN flood DoS attack. Two of the most common are the ping of death and the buffer overflow attack. The ping of death operates by sending Internet control message protocol (ICMP) packets that are larger than the system can handle. Buffer overflow attacks attempt to put more data into the buffer than it can handle. Code red, slapper and slammer are attacks that took advantage of buffer overflows, sPing is an example of ping of death.

Distributed Denial-of-service Attacks - This is similar to a DoS attack. This type of attack amplifies the concepts of DoS attacks by using multiple computer systems to conduct the attack against a single organization. These attacks exploit the inherent weaknesses of dedicated networks such as DSL and Cable. These permanently attached systems have little, if any, protection. The attacker can load an attack program onto dozens or even hundreds of computer systems that use DSL or Cable modems. The attack program lies dormant on these computers until they get attack signal from the master computer. This signal triggers these systems which launch an attack simultaneously on the target network or system.

Back door Attacks - This can have two different meanings, the original term back door referred to troubleshooting and developer hooks into systems. During the development of a complicated operating system or application, programmers add back doors or maintenance hooks. These back doors allow them to examine operations inside the code while the program is running. The second type of back door refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker. The program may allow a certain user to log in without a password or gain administrative privileges. A number of tools exist to create a back door attack such as, Back Orifice (Which has been updated to work with windows server 2003 as well as earlier versions), Subseven, NetBus, and NetDevil. There are many more. Fortunately, most anti-virus software will recognize these attacks.

Spoofing Attacks - This is an attempt by someone or something to masquerade as someone else. This type of attack is usually considered as an access attack. The most popular spoofing attacks today are IP spoofing and DNS spoofing. The goal of IP spoofing is to make the data look like it came from a trusted host when it really didn't. With DNS spoofing, The DNS server is given information about a name server that it thinks is legitimate when it isn't. This can send users to a website other than the one they wanted to go to.

Man-in-the-Middle Attacks - This can be fairly sophisticated, this type of attack is also an access attack, but it can be used as the starting point of a modification attack. This involves placing a piece of software between a server and the user that neither the server administrators nor the user are aware of. This software intercepts data and then sends the information to the server as if nothing is wrong. The server responds back to the software, thinking it's communicating with the legitimate client. The attacking software continues sending information to the server and so forth.

Replay Attacks - These are becoming quite common, this occur when information is captured over a network. Replay attacks are used for access or modification attacks. In a distributed environment, logon and password information is sent over the network between the client and the authentication system. The attacker can capture this information and replay it later. This can also occur security certificates from systems such as Kerberos: The attacker resubmits the certificate, hoping to be validated by the authentication system, and circumvent any time sensitivity.

Password Guessing Attacks - This occur when an account is attacked repeatedly. This is accomplished by sending possible passwords to an account in a systematic manner. These attacks are initially carried out to gain passwords for an access or modification attack. There are two types of password guessing attacks:

- Brute-force attack: Attempt to guess a password until a successful guess occurs. This occurs over a long period. To make passwords more difficult to guess, they should be longer than two or three characters (Six should be the bare minimum), be complex and have password lockout policies.
- Dictionary attack: This uses a dictionary of common words to attempt to find the users password. Dictionary attacks can be automated, and several tools exist in the public domain to execute them.

Well, there you have it, the only way basically to prevent these types of attacks is to get a good firewall, anti-virus software, and a good Intrusion Detection System (IDS). Tell your firewall to drop ICMP packets that will prevent ICMP flooding. I will write another article in which I will cover only TCP and UDP attacks such as:

- Sniffing
- Port Scanning
- TCP Syn or TCP ACk Attack
- TCP Sequence number attack
- TCP Hijacking
- ICMP Attacks
- Smurf Attacks
- ICMP Tunnelling

IV: E-COMMERCE IN INDIA

According to the Indian e-Commerce Report released by Internet and Mobile Association of India (IAMAI) and International Market Research Bureau) IMRB International, the total online transactions in India was Rs. 2300 crores in the year 2006-2007 (around 10 per cent of the organized Indian retail market) a 95 per cent rise over previous year's figures of Rs 1,180 crores and an over-300 per cent rise over the figures of 2004-05 (which was 570 crores). It grew by 30% to touch 5500 crores (approx by the year 2007-2008). According to a McKinsey Nasscom report the E-Commerce transactions in India are expected to reach 10000 crores by the end of 2009. [8]

Threat to E-commerce A recent survey by VeriSign, a provider of Internet security services, has revealed that at least 76% of Web users in India are exposed to online fraud and particularly phishing attacks as they are unable to identify the different forms of phishing currently happening online. [9]

V: APPROACHES IN SECURITY MECHANISM TO TACKLE ONLINE FRAUD AND PHISHING ATTACKS IN E-COMMERCE

Cryptographic techniques: Cryptography has been playing an important role to ensure the security and reliability of modern computer systems. Since high speed and broad bandwidth have been becoming the keywords for modern computer systems, new cryptographic methods and tools must follow up in order to adapt to these new and emerging technologies. Theoretical and practical advances in the fields of cryptography and coding are a key factor in the growth of data communications, data networks and distributed computing. The mathematical theory and practices of cryptography and coding is popular in providing security mechanism. There is a need to focus on other aspects of information systems and network security, including applications in the scope of the knowledge society in general and information systems development in particular, especially in the context of e-business, internet and global enterprises. [10], [11]

Paradigm of leaving and interacting: Ambient assisted living concept is envisioned through a new paradigm of interaction inspired by constant provision to information and computational resources. This provision is enabled through invisible devices that offer distributed computing power and spontaneous connectivity. A nomad traversing residential, working, and advertising environments seamlessly and constantly is served by small mobile devices like portables, handheld, embedded or wearable computers. This paradigm of leaving and interacting introduces new security, trust and Privacy risks thus support in confidence development. [12]

Language-based techniques for security: Few techniques have been implemented using programming language and program analysis techniques to improve the security of software systems. It explores and evaluates new, speculative ideas on the evaluations of new or known techniques in practical settings for solving emerging threats and important problems. It covers verification of security properties in software, automated introduction and/or verification of security enforcement mechanisms, Program analysis techniques for discovering security vulnerabilities. [13]

Compiler-based security mechanisms: This technique helps to detect host-based intrusion detection and in-line reference monitors. It also enforces security policies for information flow and access control. [14]

Group-oriented cryptographic protocols: Group-oriented cryptographic protocols are foundational for the security of various group applications, like digital conferencing, groupware, group communication systems, computer-supported collaborative work-flow systems, multi-user information distribution and sharing, data base and server replication systems, peer-to-peer and ad-hoc groups, group-based admission and access management, applications in federative or distributed environment, etc. A variety of cryptographic techniques and assumptions provides a solid basis for the design of provably secure group-oriented cryptographic protocols, which is an important and challenging task. Formal security models for group-oriented cryptographic protocols require consideration of a large number of potential threats resulting from the attacks on the communication channel and from the misbehavior of some protocol participants. [15]

Security Architectures in Distributed Network Systems:

In recent years, there has been significant increase in Internet attacks, such as DDoS, viruses, worms, spyware, and malware, etc, causing huge economical and social damage. Security Architectures in Distributed Network Systems mechanism has provided ways to attack systems in a more easy-to-use, sophisticated, and powerful way. It has greatly helped in building more effective, intelligent, and active defense systems which are distributed and networked. It has provided ways to fully understand the attack mechanisms which enables to perform effective and comprehensive defense. [16]

Key Management for Sector and File based Storage Systems: Stored information critical to individuals, corporations and governments must be protected, but the continually changing uses of storage and the exposure of storage media to adverse conditions make meeting that challenge increasingly difficult. Example uses include employment of large shared storage systems for cost reduction and, for convenience, wide use of transiently-connected storage devices offering significant capacities and manifested in many forms, often embedded in mobile devices. Protecting intellectual property, personal records, health records, and military secrets when media or devices are lost, stolen, or captured is critical to information owners. To remain or become viable, activities that rely on storage technology require a comprehensive systems approach to storage security. Key Management for Sector and File based Storage Systems techniques such as Cryptographic Algorithms for Storage, Cryptanalysis of Systems and Protocols, Unintended Data Recovery provides solutions in this scenario. [17]

Privacy and Data Sanitization: Privacy and Data Sanitization method falls within the scope of collaborative security. Any useful collaboration takes place at some point in sharing data. Unfortunately, data sharing is one of the greatest hurdles getting in the way of otherwise beneficial collaborations. Data regarding one's security stance is particularly sensitive, often indicating one's own security weaknesses. This data could include computer or network logs of security incidents, architecture documents, or sensitive organizational information. Even when the data may not compromise the data owner's security stance, sharing may violate a customer's privacy. Data sanitization techniques such as anonymization and other mechanisms such as privacy-preserving data mining and statistical data mining try to address this tension between the need to share information and protect sensitive information and user privacy. [18]

VI: CONCLUSION

Electronic commerce is growing rapidly. A number of technologies have converged to facilitate the proliferation of e-commerce. The rapid advances in computer technology coupled with rapid acceleration in communication networks and the development of sophisticated software have revolutionized the way business is done. However, this is not sufficient to proliferate e-commerce applications. With proper understanding of business needs and management of enterprise information security resources, e-commerce will mature profusely and will immensely benefit every individual. In This paper discussion of various critical part of E-Commerce and different methods avail to increase of security aspect of whole system.

REFRENCES

[1] A sengupta, C mazumdar, M s barik, e-Commerce security– A life cycle approach, Vol. 30, April/June 2005.

[2] M.M. Chaturvedi, Cyber Security Infrastructure in India: A Study, Emerging Technologies in E-Government, 2008, pp. 70-84.

[3] http://www.sans.org/reading_room/whitepapers/ecommerce/information-security-issues-e-commerce_37

[4] http://www.ecommerce-digest.com/ecommerce-security-issues.html

[5] http://www.ibm.com/developerworks/library/co-0504_mckegney/index.html

[6] e-Commerce: Business, Technology, Society (4th Edition) by Kenneth C Laudon and Carol Guercio Traver

[7] Belanger, F., Hiller, J. S., Smith. 2002. W. J. Trustworthiness In Electronic Commerce: The Role Of Privacy, Security, And Site Attributes. Journal of Strategic Information Systems, 11, 245–270.

[8] Survey conducted by Internet and Mobile Association of India (IAMAI) and International Market Research Bureau) IMRB International, 2009

[9] www.jtaer.com/documentos/CFP_trust_and_trust_management.Pdf

[10] http://www.sitacs.uow.edu.au/jucs/, Security Journal of Universal Computer Science (JUCS), Special Issue on Cryptography in Computer System, February 2008.

[11] http://www.icsd.aegean.gr/SecPerU2007, SecPerU 2007 3rd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Held in conjunction with the EEE Istanbul, Turkey, July 20,2007

[12] http://esorics2007.inf.tu-dresden.de / , ESORICS 2008 12th European Symposium on Research in Computer Security, Dresden, Germany, September 24-26, 2008

[13] http://www.cs.umd.edu/~mwh/PLAS07/, PLAS 2007 ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, San Diego, CA, USA, June 14, 2009.

[14] http://www.dfrws.org/ , DFRWS 2007 7th Annual Digital Forensic Research Workshop, Pittsburgh, PA, USA, August 13-15, 2007.

[15] http://www.hgi.rub.de/gocp09/ , GOCP 2007 1st International Workshop on Group-

Oriented Cryptographic Protocols, Held in conjunction with the 34th International Colloquium on Automata, Languages and Programming (ICALP 2009), Wroclaw, Poland, July 9, 2009.

[16] http://nss2008.cqu.edu.au/ , NSS 2008 IFIP International Workshop on Network and System Security, Dalian, China, September 20, 2008.

[17] http://ieeeia.org/sisw/2005/, SISW 2005 2nd

[18] International IEEE Security in Storage Workshop, San Diego, California, USA, September 27, 2005.

[19] http://www.trustcomp.org/secoval/, SECOVAL 2007 3rd Annual Workshop on the Value of Security through Collaboration in cooperation, Held in conjunction with the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm 2007), Nice, France, September 17-21, 2007.