IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 43-46

E-Commerce Security

NileshKote , Pratik Deshpande
TulsiramjiGayakwadPatil College of Engineering and Technology,Nagpur

Abstract: *E-commerce (electronic commerce) or EC is the buying and selling of goods and services, or the transmitting of funds or data, over an electronic network, primarily the internet. When a buyer pays with a bank card swiped through a magnetic-stripe-reader, he or she is participating in e-commerce. E-commerce Security is a part of the Information Security framework and is specifically applied to the components that affect ecommerce including of Data security and other wider realms of the Information Security framework. 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. Ecommerce offers the banking industry great opportunity, but also creates a set of new risks and vulnerability such as security threats, hackings. Therefore it is an essential management and technical requirement for any efficient and effective Payment transaction activities over the internet. Due to the constant technological and business change and requires a coordinated match of algorithm and technical solutions. In this paper we discussed with Overview of security for ecommerce, various steps to place an order, Security purpose in E-commerce, various security issues in E-commerce, guidelines for secure online shopping etc.*

I. Introduction

The eradication of trust in Internet commerce applications may cause prudent business operators and clients to forgo use of the Internet for now and revert back to traditional methods of doing business. This loss of trust is being fueled by continued stories of hacker attacks on e-commerce sites and consumer data privacy abuse. Hackers demanding a ransom from an ecommerce site for not publishing customer credit card information have increased the visibility of the network security weaknesses in most business institutions. The conflict between convenience and ease-of-use vs. security has always been resolved in favor of convenience.The thieves were stealing bills, paychecks and other consumer identity related mail from the victim's home mailboxes or from the postal system's street mailboxes. This type of security breach happens much more often than one in which a thief steals directly from inside a post office. Security standards, controls and practices have been developed within the main trunks of the postal infrastructure to monitor and hopefully prevent mail interception or tampering when the letter is in the system. Similar controls are in place at the equivalent Internet network level. Controls at the endpoints on the other hand vary widely from very good (usually at the originating business) to non-existent (usually at the home computer).

Consumer privacy is becoming the most publicized security issue replacing theft and fraud as top concerns in e-commerce. The DDOS attacks demonstrated that business sites did not maintain adequate security protection and intrusion detection measures. Some of the sites did not detect the compromise, which occurred months before the DDOS attacks. No customer will want to use a business that distributes sensitive customer data such as credit card information, SSN information or credit limits without the knowledge or permission of the customer. Is this situation different from similar abuse in the phone or mail order business model? Not really but the major difference has to do with the speed of access to and dissemination of the sensitive data.

User and system administrator awareness is becoming more important in the effort to counter e-commerce attacks. Consumers are slowly becoming aware of some security features such as encrypted WEB transactions, privacy statements by companies, etc. Internet service providers are becoming more responsive to complaints about Internet abuse originating from their sites.

E-commerce security needs to be addressed not only at the business site with its servers/network but also on the client side, which includes direct connected home computers. It is this group of computers that are the most vulnerable to attack because the level of user security training or awareness is not high at all.

The Threats to E-Commerce

The standard client server model has three components: the server system, the network and the client system. In the past, server systems were typically mainframes running operating systems such as MVS, VM, VMS or Unix. Window NT and Windows 2000 (W2K) arenow making inroads into this arena. The network component includes the internal business network, the path between the business and the customer through various ISPs and the customer's internal network. Client systems are usually PC or Macintosh systems running

their respective Window 9x, NT, W2K or MacOs operating systems although Unix systems do serve as client systems.

. E-commerce Security Components

E-commerce security strategies deal with two issues: protecting the integrity of the business network and its internal systems; and with accomplishing transaction security between the customer and the business. The "ILOVEYOU" virus successfully penetrated firewalled networks because inbound and outbound email is allowed to pass through the firewall. The Code Red and NIMDA worms passed through firewalls because they accessed systems through the standard WEB server ports. Transaction security depends on the organization's ability to ensure privacy,authenticity, integrity, availability and the blocking of unwanted intrusions . Transaction privacy can be threatened by unauthorized network monitoring by software devices called sniffer programs. These programs are most likely found at the endpoints of the network connection. There are a number of defenses against this threat such as encryption and switched network topologies. Transaction confidentiality requires the removal of any trace of the actual transaction data from intermediate sites. Records of its passage are a different thing and are required to verify the transaction actually took place. Intermediate nodes that handle the transaction data must not retain it except during the actual relaying of the data. Encryption is the most common method of ensuring confidentiality. Transaction integrity requires methods that prevent the transactions from being modified in any way while it is in transit to or from the customer. Error checking codes are an example of such a method.

Viruses

Viruses are the most publicized threat to client systems. They are effective because of the built-in insecurity of client systems (PC/Mac). Subverting a PC/Mac system requires access to the system and no special privilege is needed to write code or data into sensitive system areas. This operating system design issue is evident in older versions of Windows 9x or MacOs 8.x. Operating systems such as Windows NT, Windows 2000, while still vulnerable to thistype of attack, do have the capability of restricting who can activate the virus. The more publicized viruses such as Melissa, ILOVEYOU, Resume, KAK and IROK have no effect on Unix systems. Viruses need "system privilege" in order to be effective. In general, the multiple privilege access schemes present in Unix, VMS and other multi-user operating systems prevents a "virus" from damaging the entire system. It will only damage a specific user's files.

Trojan Horses

The BackOrifice, Netbus, BO2K hacker tools allow a remote user to control, examine, monitor any information on the target PC. There are commercial tools like CUCme, VNCviewer that perform the same function. There are numerous hacker exploit web sites such as www.portwolf.com/trojans.htm, www.cultdeadcow.com, www.rootshell.com, http://thc.pimmel.com and www.insecure.org where anyone can download a copy of the abovementioned Trojan horse programs. The good side of the Force allows system administrators to use these tools to remote manage large numbers of workstations. This is the typical sysadmin support tool since there are many more machines than sysadmins. The hacker has full control of the victim's computer. The hacker can move the mouse and run any program, modify any file or delete any file from the victim's system. In addition, the hacker can see everything that the victim does on his computer. These types of programs become more dangerous to e-commerce than viruses as more direct connect households enter the Internet with little or no protection from this type of attack. Thus the purveyors of e-commerce must find ways to provide the tools and change the culture of personal computing in order to tighten security at the client endpoints.

Privacy Issues

The abuse of consumer privacy is becoming a concern at the consumer, business and government level. There will be resistance to participating in certain types of ecommerce transactions if the assurance of privacy is low or non-existent.

Abusing Customer Privacy

The government (Big Brother) isn't the biggest threat to privacy anymore. Businesses are. The bank supplied a telemarketer, MemberWorks, with sensitive customer data such as name, phone #, bank account and credit card numbers, SSN, account balances and credit limits. MemberWorks used these customer lists.to sell dental plans, videogames, and services. US Bankcorp settled out of court. Well Fargo, Bank of America and other financial institutions announced they were discontinuing the practice after the US Bankcorp settlement was announced. Many banks still deal with MemberWorks today. Jane Bryant Quinn's essay on Privacy Issues [3] lists a couple of items of concern:

1. No Federal law shields “transaction and experience” information.
2. Social Security Number information is periodically disclosed either intentionally or not.
3. Self-regulation by business doesn’t work.

Obviously, not all businesses are dens of information disclosure. However, most businesses do not treat the information security cycle as a high priority until an event happens. They consider a firewall to be the best line of defense and pay not enough attention to securing the internal net.

The Distributed Denial of Service Attacks (DDOS)

Businesses that rely on web-based transactions are and will continue to be vulnerable to Denial of Service (DoS) attacks. DoS attack scripts are the most common, effective and easiest to implement attacks available on the WEB. No actual damage is done to the victim site.

The access paths to it are simply overwhelmed with incoming packets. It would be every businessman's dream to be in this situation if the incoming packets were legitimate customer orders. However, it can be their worstnightmare if they are the targets of a DoS attack.The 1999 DDOS attack against the University of Minnesota generated over 2 billion packets sent from under 300 systems in 10 minutes.

The DoS attack is diabolically simple. Every packet transmitted on the Internet contains a source and destination address. The simplest example is that of a ICMP ping transaction. The basic transaction is:

1. source system sends a "ping" packet to the target. This is an ICMP_ECHO_REQUEST packet containing the source address of the sender and the target address of the receiver.
2. If the target system is able to respond, it sends a response back to the source address listed in the "ping" packet. This is an ICMP_ECHO_REQUEST_REPLY packet.

The E-commerce Site’s Security Responsibility

DDOS attacks worked because sites failed to detect the initial compromise of their systems. The compromises could have been prevented if standard system maintenance had been performed.

E-commerce sites need to tailor their security architecture to meet the demands of ensuring consumer data privacy and that company resources are not used to attack other Internet sites. A business can certainly survive the publicity generated if their network is used to attack another site. It most certainly wouldn't survive if word gets out that customer credit, purchase, or personal data is stolen or copied without their knowledge or permission. For example, a hacker broke into an Internet music store, CD Universe, and published 300,000 customer credit card numbers when the store refused to meet his extortion demands [13]. This action prompted major credit card companies to issue replacement cards for the customers affected by the attack. It suffered another blow when the security investigation revealed that the security hole was well known and that a vendor patch was available to close the hole. The hacker could have easily mounted a data integrity attack on CD Universe's customer database instead of demanding a ransom.

Software developers need to design software that is engineered for safety and security. It isstill possible to add ease-of-use features but they should be initially turned off.

Proper training programs for the system administrators are the easiest and most effective way to prevent major security compromises. The Audit group needs to review the security methods to ensure their compliance with company policy and general Internet security standards.

The Client Responsibility

Cable modems, DSL connections and other high speed direct connect mechanisms for connecting to the Internet create an entirely different set of security issues. The migration of DDOS attack tools to the Windows OS now allows a hacker to use these direct connect systems as another base of operation. The ISP’s responsibility to maintain network integrity and create a model for containing any attack with their domain is paramount. There are a number of documents available to these ISPs that provide guidelines for securing their networks [14].

The estimated number of systems used in the original DDOS attacks of early 2000 is thought to be less than 1000. There are certainly orders of magnitude more direct connect systems with minimal security tools installed. Certainly, the system administration expertise of these systems is not very high.

The client's main responsibility deals with requiring ecommerce sites acknowledge the right of the customer to examine their credit history and to be provided with information about who gets that information. Ecommerce businesses should develop orientation programs for their customers that teach about basic security practices. This certainly helps ensure confidence in the business' ability to secure and protect the customer information.

II. Conclusions

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.

Trojan horse programs launched against client systems pose the greatest threat to e-commerce because they can bypass or subvert most of the authentication and authorization mechanisms used in an e-commerce transaction. These programs can be installed on a remote computer by the simplest of means: email attachments. Training programs, orientation programs will become more critical in order to increase the general populace's awareness of security on the Internet.

IT and financial control/audit groups within the ecommerce site should form an alliance to overcome the general resistance to implementing security practices at the business level.

Industry self-regulation of consumer privacy appears to be ineffective. The FTC privacy survey and its recommendations to Congress may result in the introduction of legislation on privacy issues.

References

[1]. Randy C. Marchany, Tom Wilson. A Keystroke Recorder Attack on a Client/Server Infrastructure. Proceedings of the Network Security '96 Conference, SANS Institute

[2]. Peter Keen. Ensuring E-Trust.ComputerWorld, 3/13/00 issue Jane Bryant Quinn. The Spies in Your Pocket". Newsweek, 8/16/99

[3]. Northcutt, Cheswick, Kent, Cooper, Marchany et al. Consensus Roadmap for Defeating Distributed Denial of Service Attacks. www.sans.org/ddos_roadmap.html

[4]. "Distributed System Intruder Tools - Trinoo and Tribe Flood Network", Computer Incident Advisory Capability, Lawrence Livermore National Laboratory, CIAC 00.040, 12/21/99

[5]. Patrick Thibodeau. Privacy Concerns Rankle Industry – In Blow to sites, FTC pushes for regulation. Computerworld, 5/29/00, Vol 34.no 22.

[6]. "Lucrative mail theft on the rise", RoanokeTimes reprint of LA Times article, 6/1/00

[7]. Ravi Kalakota, Andrew B. Whinston. Electronic Commerce: A Manager's Guide, Addison-Wesley, ISBN: 0-201-88067-9

[8]. William Safire. The Phantom of the Internet. New York Times Service, article appeared in 6/4/00 issue of the Roanoke Times.

[9]. The SANS Institute, www.sans.org/topten.htmThe Internet Audit Project, http://www.securityfocus.com/templates/forum_message.html?forum=2&head-32&id=32

[10]. www.detached.net

[11]. www.usatoday.com/life/cyber/tech/cth186.htmwww.sans.org/dosstep/index.htm