International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 4, July - August 2015 **ISSN 2278-6856**

E-commer Security Issues and Proposed Security Model For Online Transaction

Prof. (Dr.) Prashant P. Pittalia

MCA Department, SJPIBMCA Gandhinagar, Gujarat

Abstract

Most of the E-commerce websites provide their customers to remotely do any transaction and be safe from Internet attacks. For any business either it is business-to-business, business-to-consumer, consumer-to-consumer or business-to-government it is needed that they exchange the information with secure manner. Business needs proper implement of the security services like authentication, confidentiality, integrity, access control and non-repudiation with the use of proper mechanism like encipherment, notarization, authentication exchange, routing control, digital signature. The paper explains the usefulness of E-commerce security model for the Organizations which are doing their business online. The proposed E-commerce security model provides the rules that inform how system should configure and user of an E-commerce website should act in normal situation.

Keywords: Authentication, acquire, payment gateway

1. Introduction

Electronic disasters can ruin businesses, sink careers, send stock prices plummeting and create public relations nightmare. For responsible organizations operating in the age of electronic communication and E-commerce, a proper security model is an essential to protect & make transaction secure. A secure model for E-commerce website is one of the best ways for employers to protect themselves from workplace lawsuits and other risks associated with the inappropriate use of corporate software, Email and Internet systems. The consequences of insecure authentication in a banking or corporate environment can be disastrous, with loss of confidential information, money, and compromised data integrity. Many applications like banking, healthcare, immigration and border control, etc require user authentication, including physical access control to offices or buildings,. The Proposed security module provides the solution for the said problems with the help of biometric authentication techniques.

2. E-commerce Security Issues

The potential growth of e-commerce depends on people believing that surfing the Internet and buying and selling online are safe activities that will not result in financial loss or an invasion of privacy. The TCP/IP protocol used to transmit data over the Internet was not designed to be secure, which means that data transmitted from computer to computer can be intercepted, read, and even altered. The important issues related to E-commerce security are described as follow.

2.1Hacking

Hacking in simple terms means illegal intrusion into a computer system without the permission of the computer owner/user. However, in practice, hackers generally have a particular target in mind, so their unauthorized access leads to further acts, which national law might also define as criminal activities.

2.2 Virus Dissemination

Malicious software that attaches itself to other software. (Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious softwares). Now a day's most of the computer user uses the pen drive to store the personal information and secret documents. It is most frequently use to transfer the information. Most of the people do not know is there any harmful software running in their pen drive or not. They use it at different places in spread the malicious software very easily without knowing about it.

2.3 Denial of Service

DoS is much like attacks that limit all traffic into a site, including legitimate traffic. When attacked, it is difficult for victims to gain access to their systems or to filter out bad traffic. This is often a serious crime, especially when a company may be forced to go out of business because of it. This has been true in the past when ISPs were forced off the Internet by a DDoS attack for a series of days. They were unable to meet their SLAs (Service Level Agreement) and were forced to shut down.

2.4 Credit card fraud

Many attackers are money focused, with a financial incentive for an attack, and so target their attacks on databases containing many credit card numbers. Attackers are likely to target credit card processors and transaction clearinghouses, since they deal in a large volume of credit card numbers daily. You simply have to type credit card number into www page of the vendor for online transaction If electronic transactions are not secured the credit card numbers can be stolen by the hackers who can misuse this card by impersonating the credit card owner. Sometimes the false slot is fixed at ATM machine, which uses the same color, and sticker of the original card slot. It contains the additional card reader to copy your card information and then after using the duplicate card to perform illegal transactions. Sometimes the pamphlet holder is put near to the ATM machine with the micro camera in it. The micro camera can set in such a way that it can view the KEYPAD and also send the screen on monitors up to 200 meters. On March 20, 2009, A BBC sting operation has exposed a criminal gang in India that sells credit card details of UK customers, reportedly stolen

from call centers in India. This gang was sold the credit and debit card details at $10 a card.

2.5 Damage of Data and Code

Most organizations now depend to some extent on computerized information systems, and any act resulting in significant corruption or deletion of corporate data could have serious implications on their ability to transact business. Companies and individuals depend on the integrity of the data that they access from the Internet. For example a customer will make a purchasing decision based on the price shown on a web page. If this price has been altered because of a security breach, the online company could risk losing money, the customer, or both. A company could access its website one morning to find a competitor's address in place of its own. Another form of vandalism occurs when an individual attempts to crash computers and servers by sending huge files or thousands of messages to the same email address at once.

2.6 Wi-Fi Hacking

Most computers built during the past five years come with Wi-Fi built in and usually enabled in the promiscuous mode; this means that a savvy hacker can set up a Wi-Fi access point nearby and cause this Wi-Fi enabled computer to dutifully connect to that rogue access point. The access point's operator can then easily add, remove, or modify files in the targeted computer, even if that computer's owner never consciously connected to the Internet.

2.7 Silent Intrusion

Cyber criminals gain access to systems without authorization and without setting off any detection devices. This is often the most nebulous type of intrusion, since the victim is unaware of the presence of an unauthorized user who may be there to collect data via key loggers and Trojan horses. The purpose of this type of access is specifically passive and is mean to allow the attacker to maintain long-term- access.

2.8 Salami Attack

In such crime criminal makes insignificant changes in such a manner that such changes would go unnoticed. Criminal makes such program that deducts small amount like Rs. 0.50 per month from the account of all the customer of the Bank and deposit the same in his account. In this case no account holder will approach the bank for such small amount but criminal gains huge amount.

2.9 Cyber Stalking, Defamation

The Criminal follows the victim by sending emails, entering the chat rooms frequently. The Criminal sends emails containing defamatory matters to all concerned of the victim or post the defamatory matters on a website. (Disgruntled employee may do this against boss, ex-boys friend against girl, divorced husband against wife etc)

2.10 Software Privacy

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. Retail revenue losses worldwide are ever increasing due to this crime. It can be done in various ways like End user copying, Hard disk loading; Illegal downloads from the Internet etc.

2.11Spoofing

Getting one computer on a network to act as if to have the identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network.

2.12 Loss of Data

If you loss data, you loss customers and control, opening yourself up to possibilities for fraud. You could loss data for physical reasons (hard drive crashed), because you were hacked, or because you were careless. Loss or unauthorized use of data can be attributed to three causes: theft, fraud, and human error.

3. PROPOSED SECURITY MODEL FOR E-COMMERCE WEBSITES

The proposed model differentiates the responsibilities of parties involved in E-commerce payment transaction processing. The parties associated with a payment transaction cycle are Card Issuers, Card Holders, Card-Acquirers and Merchants. The Merchant have close relation with Card-Acquirers. The Cardholders have close relationships with Card Issuers. The Model defines the following three domains.

3.1 Issuer Domain

An issuer is a financial institution that maintains the relationship with cardholder. It issues cards to its cardholders for payment of online transaction. A cardholder is an authorized user who uses a web browser to interact with e-commerce merchant's site for online purchase. The issuer is responsible to enroll the cardholders in the service by accepting the biometric information; verify the identity of each cardholder who enrolls, and authenticate cardholders by their biometric information during online purchases. The issuer system handles communication with merchants and a centralized directory, which acts as a communications intermediary between the Merchants and Issuers.

The software deployed by the issuers needs to be integrated with their back-end card systems providing access to cardholder information. After the enrollment of cardholder on issuer site, he/she does not need to install any specific software on their side. They have to just use a standard (SSL enabled) browser to conduct their transactions.

3.2Acquirer Domain

An acquirer is a financial institution that contracts with merchants to accept and process cards for payment of goods and services. An acquirer is often referred to as the "merchant bank". The Acquirer is responsible for defining the procedures to ensure that merchants participating in Internet transactions are operating under a merchant agreement with the Acquirer. In short, Acquirers are responsible for deploying a payment gateway and Merchants install the payment gateway plug-ins, along with a Merchant Plug-in (MPI) provide by ePayments Services provider, to handle communication with the Central Directory and Credit Card Issuer.

As the cardholder enrolled them to card Issuers, their biometric information is transferred over the Access Control Servers (ACS). The Directory is an Internet based Directory, providing lookup information on participating credit card Issuers and the location of their Access Control Servers (ACS) on the Internet. The ACS's help in authenticating the card-holders based upon pre-registered information provided by cardholder during the time of enrolment. Merchants communicate with the Directory through ePayments Services provider, in order to provide authenticated transactions. The Payments Technology Company Directory utilizes the normal Payments Technology Company Network communication channel between Issuers and Acquirers for credit card authorizations.

3.3Interoperability Domain

Payment technology company Network is a collection of systems that supports the electronic transmission of all card authorization between acquirers and issuers and facilitates the settlement of funds. Interoperability Domain is responsible for exchange of E-commerce transactions between the Issuer and Acquirer with a common protocol and the Payments Technology Company Directory and Network.

3.4Model Desing and Operations

The Model contains two main functions Enrolment and Authentication.

3.4.1Enrollment

Through the use of enrolment process cardholders are enabled to use the Secure Services. When cardholders enroll, they are asked for biometric data and personal information like a password and a Personal Assurance Message. After collecting this data and verified by the Issuer, the card holder is considered to be enrolled in secure methodology.

The Enrolment Server passes the record of enrollment to the Issuer's Access Control Server. In future whenever the cardholder conducts an E-commerce transaction on Merchant website for payment, a secure authentication request is generated and Access Control Server will be queried to certify that the cardholder is in fact enrolled in Secure Model.

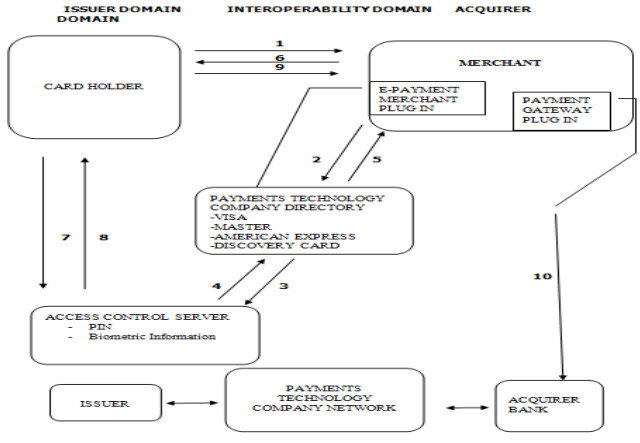

Figure 1. Model for secure transaction

Steps involved in a enrolment process

Cardholder goes to Issuer website for the registration and then he/she goes to enrolment web page and provides card details and other identification information specified by the Issuer and biometric data such as (fingerprints, face, voice, signature and iris) that he/she wants to use for secure transaction.

Issuer Validates Cardholder personal and biometric information and notifies the cardholder of successful completion of the enrolment process.

Enrolment Server then sends the confidential data to the Access Control Server (ACS), including the newly enrolled card number and biometric data required for subsequent purchase authentication.

3.4.2Authentication

After enrolment, the cardholder is allow to shop at any participating merchant site where the merchant is enabled by integrating his/her site with Merchant Plug-In, which the merchant can obtain from a ePayments Services provider. The Merchant Server Plug-in obtains the cardholder information and is able to access the Issuer's Access Control Server to validate the cards participation in the service.

After the cardholder clicks "Buy" or "Check-out", the MPI (E-payment service provider) sends a message to the Payment technology company directory containing the cardholder account number. Through an exchange of messages, the Payment technology company Directory and the Access Control Server (ACS) determine if the cardholder is enrolled in secure service. A message is returned to the Merchant Server plug-in, indicating the result. The MPI then sends an authentication request to the Access Control Server (ACS) through the cardholder's browser and the Access Control Server performs the biometric authentication routine defined by the Issuer; e.g., it may demand for fingerprints, face, iris, signature, voice etc., as the case may be. The Access Control Server now sends the results of the authentication to the Merchant Server Plug-in. If this response from the Access Control Server indicates successful authentication, the MPI returns the successful authentication response to the Merchant and the transaction is processed as usual.

Steps involved in an Authentication process

The Cardholder clicks on "Checkout" button at the Merchant site in shopping cart and enter the card number and clicks "OK".

The MPI queries the Directory Server for Issuer Participation and sending the card number. The Directory server queries appropriate Access Control Server to determine whether the authentication is available for the card number. ACS responds to Directory Server. Directory Server forwards ACS response to MPI.

The MPI sends Cardholder authentication request to the Access Control Server through Cardholders browser where he/she use the biometric device to provide the one of biometric value.

The ACS challenges the Cardholder for his/her biometric data then verifies it and returns the authentication to the

MPI via the Cardholder's browser and copies the same to the Authentication History Server.

The MPI validates the response, and depending on a successful response, Merchant proceeds with authorization exchange with its acquirer.

4. BENEFITS OF E-COMMERCE SECURITY MODULE

The primary benefit of E-commerce Security Module is the reduction in disputed transactions and the resultant exception handling expense and losses. It is expected that nearly most of all e-commerce charge-backs, and a substantial proportion of customer complaints, could be eliminated with the use of Authenticated Payment. This will have a positive impact on Merchant profitability. The main benefit to the Issuing Banks is that they can provide assurance to their cardholders who are doing their e-commerce transactions.

- •Increased consumer confidence so sales will be increase.
- •Reduced cardholder disputes, charge backs and associated handling cost
- •Globally-supported service
- •Utilize secure socket layer (SSL/TLS) encryption

4.1 Benefits for Merchants

1. Customers confidence increase for online purchasing as well as increased sales
2. Customers and Merchant interaction is not affected the system.
3. The chances of the fraudulent transactions will be reduced.

4.2 Bneefits for Cardholder

- Increased consumer confidence when purchasing on the Internet. The consumer is ready to provide their detail without fear of steel the data because without biometric authentication no one can utilize their card details as well as personal details.
- Control over card used for online purchase.

4.3 Benefits for Issuer

- Because Identification of a customer through only biometric characteristics, which reduce the fraudulent transactions
- When the consumer do the transaction issuer is involved and validate the biometric information provides by the consumer. The Issuer and Consumer relationship become stronger, which helps Issuers to make it popular.
- Provides Issuers with the opportunity to leverage existing cardholder authentication techniques such as those used for their online banking services
- Consumer of Issuers do not required to Install a special software for that they need just browser for E-commerce transaction.

4.4 Benefits for Acquirer

- Reduced the disputed transactions and Increase the Merchant sales.
- Major problem of charge backs in the E-commerce transaction is most probably reduces.

5. CONCLUSION

Organizations which are doing their business online wants to use the E-commerce security model which provides proper functioning and monitoring of online activities with less effort. Here I have discussed what work should be include/exclude in E-commerce security model. The proposed steps for the secure model are helpful for E-commerce sites. The proposed E-commerce security model is utilized by Academic Institutions, Government Organizations or any individual group or company as per their requirement. The problems on e-commerce websites for doing transaction is solved with the help of the proposed model. This model facilitates the consumer to protect their confidential information with the help of biological characteristics.

References

[1.] Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Eric D. Knapp, Joel Thomas Langill, Syngress

[2.] DNA: World, "Credit card details of Britons sold at $10 each", Mar 20, 2009, http://www.dnaindia.com/world/report_credit-card-details-of-britons-sold-at-10-each_1241063

[3.] Securing information and communications systems: principles, technologies, and applications, Steven Furnell, Sokratis Katsikas, Javier Lopez, Artech House,

[4.] Security Week News, "Database Admin Sentenced to 12 Months in Prison for Hacking Former Employer's Network", July 06, 2010, http://www.securityweek.com/database-admin-sentenced-12-months-prison-hacking-former-employers-network

[5.] Spring 2009:"Computer Networking Project", http://www.lsumter.info/ComputerNetwork

[6.] Computer Security: Concepts, Issues & Implementation, Alfred Basta & Wolf Halton, Cengage Learning,

[7.] Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Eric D. Knapp, Joel Thomas Langill, Syngress

[8.] Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Eric D. Knapp, Joel Thomas Langill, Syngress

AUTHOR

Dr. Prashant P.Pittalia, [Ph.D., MCA, M.Sc.(PHYSICS)], Associate Professor in MCA Department at SJPI, Gandhinagar, having 15 years of teaching experience in computer science. He has expertise in E-commerce Security, Cyber Security, and Socket Programming etc