Security threats to e-financial transactions essay

ASSIGN BUSTER

Internet security is very essential in electronic commerce where financial transactions are taking place. It might seem to a normal user that it is very difficult for a hacker or a cracker to see the financial information being sent over the internet. In fact, it is a lot easier for a cracker or hacker to see the information being exchanged if the system or connection is not secured or encrypted.

A cracker requires a very few resources and some computer skills to steal a user’s financial information that is being exchanged over the internet. Hence these security threats need to be addresses to provide users secure connection and reduce these threats. Electronic financial transactions refer to the exchange of money over the internet with the help of a financial intermediary. This transaction requires at least two parties to be involved in a transaction where one is a merchant and other is the buyer.

The financial transactions over the internet can also be made with the bank, where there is only one user. Online banking is a typical example of this type of financial transaction over the internet. The attacker is also one of the players in this exchange of money over the internet. The attacker or cracker can strike the merchant, the intermediary party or/and the buyer and their resources with damaging schemes that can cause the exploitation of the system. Most of the security threats over the internet are classified as availability, integrity and confidentiality. A security threat is a possible strike of the cracker against the system for his gains or just for fun.

The statistics show that United States received most of the e-commerce attacks from crackers in the past few years. The users of the internet or the

people engaged in online transactions mostly fear the theft of their credit card information. Unless there is a secure connection over the internet, it is very easy for a cracker to steal the credit card information, when it is being sent over the internet. This not only limits the online transactions but also prevents the users to use the credit card for making online payments. However, according to the CyberSource Corporation, around only 2% chances of credit card fraud exist in reality.

This was a great threat a few years back when there were no laws for e-commerce and no concept of secure transactions existed. The nature of this type of threat is the theft of personal information and it attacks the confidentiality of information and the authenticity of the user. The threat is not so severe today however, if a cracker gets hold of credit card information of a buyer, he can make a fortune of it. Today, in order to encourage the transactions over the internet, the federal laws protect the consumers in many ways.

In most of the cases, where the amount of theft surpasses US$ 50, the credit card company is held responsible for payments and in some cases the merchant is liable to pay the amount if he is unable to verify the account. The other way in which these frauds are avoided is through the identity verification mechanisms. The use of digital signature allows the merchant and the bank to be sure about the authenticity of the user’s identity. A secure connection is developed for the exchange of credit card information over the internet to minimize these losses.

This is mostly performed using an eavesdropping program that can monitor and record any information being sent over a network. When used for criminal intent, sniffing can have grave consequences over the user and the merchant. Sniffing software allow the hackers to steal information from anywhere on the desktop or from the network including any instant messages and confidential information placed at desktops. The major threat of sniffing is that the confidential information of a user or merchant can be made public. Hence the confidentiality and privacy of the users are the major risks. The information such as financial account numbers can be stolen over the network when exchange is made over the internet.

The threat is pretty severe because that account number can be used to transfer all of the funds in an account to another account (Techi Warehouse 2010). Sniffing is a passive attack that does not hamper any communication between the merchant and the user. Mostly, these types of attacks are made on the lower networking layers. Email Wiretap is one of the varieties of sniffing threats. In this threat, the hacker can write a hidden code in an email message that allows the succeeding messages to be forwarded with the original email.

Any information being exchanged over the internet and over email messages can be stolen by the hackers using sniffing software. Sniffing can be addressed by the use of Secure Socket Layer or the SSL protocol which encrypts the data being sent over an unsecure network. The data is encrypted when it leaves the shopper’s computer and is decrypted when it reaches the system of the merchant. Whenever SSL network is requested,

the browser will identify the website as a trusted one and hence it will enable the handshake to send the information in encrypted form (IBM 2005).

A Certification Authority issues certificates for SSL connections to the businesses and hence the business is authorized by the govrnement. When the shopper’s desktop makes a request, it first checks if the site owns a certificate or not. If not, then it notifies the user about it and asks for the permission to go forward or not. Hence the hacker who is trying to sniff the contents of this exchange will not be able to read the data.

However, this only addresses the problem of integrity of data. Spoofing is the sending of emails which are intended to appear as if they were sent by someone else. The actual source of the email is hidden from the receiver and the receiver thinks it is from some other source. Pishing is similar to spoofing and it is the dissemination of email with a false declaration of being a registered business (Techi Warehouse 2010).

The aim of this type of threat is simply to provoke the receiver to engage in some sort of information exchange that can be used by the hacker. This threat can prove to be dangerous is some sensitive data is sent by the receiver to the hacker upon receiving this email message. If the hacker has done his homework and made the look and feel of the email similar to some legitimate business’s, then the receiver may be deceived (Laudon 2008). Through the use of spoofing and pishing, the attackers can obtain some property or money from the users in a fraudulently manner. These frauds include sending bills, charges and trying to obtain money from the user by intimidating him and making him believe that the bill sent is the real one.

Investment frauds and in debt elimination schemes are a part of these pishing techniques where the hacker tries to obtain money from the receiver by fooling him. The category of these crimes is identity theft and if successful, the hackers can make a lot of money by fooling a number of online users. Mass marketing by the hackers is also a form of spoofing and pishing where the hacker poses to be a business selling products online. The users think that it is a legitimate business and hence they engage into some form of electronic transaction with this hacker. Hence they provide the hacker with their credit card number, checking account number of transferring the money to the account of the hacker. The use of Digital Certificates has eased the problem of authentication as most of the businesses using electronic transactions have certificates from Certificate Authorities who ensure that each user has a unique certificate.

INSIDER ATTACKS Although many users think that most of the major security threats come from the external source, but the fact is that the internal sources are as much unreliable as the outsiders. The most severe financial security threats come from the inside of an organization rather than the outside. Bank employees are able to steal far more information and money than the crackers. Employees have access to some very sensitive and essential data about the customers that can be manipulated and in cases of even minor deficiency of internal security these employees can do anything with that information for their benefit (Laudon 2008).

Citibank confirmed in September 2007 that its employees were involved in some data breach that was being investigated. This breach involved the credit card information, the names and the social security numbers of

thousands of Citibank customers. This information was used by ABN Amro Group’s employee and shared onto the Limewire file sharing software (Laudon 2008). Another instance of an insider job that happened in a bank was by Nadeem Kashmiri of HSBC bank in the global services center in Banglore. He was one of the employees in the trusted list of this British financial services bank and his actions were deeply condemned by the bank.

Nadeem was accused to illegally diverting the some portion of funds of the private accounts of clients of HSBC to his account. The fraud was caught by the security team of HSBC and after investigations it was uncovered that only some United Kingdom based clients were affected and their losses were reimbursed fully. However, Nadeem was able to make a lot of money out of this act because a number of accounts of the private clients were involved and even if a small amount of money was diverted, then also a large sum of money could have been made (Fernando 2009). These occurrences can be avoided by the strict use of access controls in the working environment and keeping the data of the customers as safely as possible.

The employees even on trusted list should not be able to see the information of the clients such as their account numbers or social security numbers. Auditing of the employees’ financial records and their personal accounts might also help and avoid such occurrences. Another solution might be to store the information in encrypted form in the databases that no one can access. Only those allowed can access this type of confidential information.

Transaction Authentication System (TAS) can be used to tackle the problem of insider attacks that uses the Automated Banking Certificates in its

infrastructure. In this infrastructure, the primitive cryptographic techniques are used to identify the user and authenticate the data. However, the main part of TAS is an audit agent that gathers all the required information and verifies the relation between any audit trails (Corzo, et al. 2006).

The new technologies and the e-commerce laws have reduced the actions of hackers and crackers over the internet. However, the threat is still there as the above mentioned defenses are not 100% fool proof. The use of Public Key Encryption and the use of Digital Certificates have solved the problems of authentication and confidentiality. The companies, whose businesses depend upon the electronic transfer of money, have invested a lot of money in the security of the transactions.

In United States, US$ 8 billion were spent by the businesses to enhance their businesses.