Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Addressing Information Security and Implementations to Check Internet Security Threats

[1]Dr.Anurika Vaish, [2]Aniruddha Singh, [3]Saurabh Srivastava*,[4]Amritanshu Kalia
[1]Professor ,MS/MBA Department, India
[2, 3,4]M.S. in Cyber Law & Information Security, India
[1,2,3,4]Indian Institute of Information Technology, Jhalwa, Allahabad, India

***Abstract:** In traditional transactions, the coins and currency notes were the common modes of money exchanges. Later on this system shifted to manual banking mode. A traditional user is always paranoid of safety of real (physical) money. In case he uses the bank facilities then he has to go to a bank for opening an account, to get the cash, to get a cheque book issued and getting a draft prepared. But the advancement in electronics and computers has completely changed the scenario of traditional dealing. Caring for safety of physical money or going physically to a bank are bygone stories. Now deals can be carried out by sitting at home and without going to a bank. Opening of an account, purchases and sales, to and fro payments; all can be done through electronic means. These activities can also be performed the world over by adopting a bank which is member of SWIFT (society for Worldwide Interbank Financial Telecommunication). The digital currencies and electronic payment systems have made the business activities much easier than before. The days of paper bulks, their tedious handling, and risk of getting ruined are over. Now everything is in computer memory. Any business record can be searched in minimum time which was rarely possible in traditional business. The security of documents has also increased which was always vulnerable in traditional business.*

***Keywords:** Internet security, E-commerce, Cyber crime, Data Encryption*

1. Introduction

Need of money for a business, in the evening or night (non-banking hours), was not possible through traditional banking means. But the **ATM** (Automatic teller machine) has made it so. Now money can be withdrawn any time in 24 hours. Thus the business facilities have also become non-restrictive to both: the buyer and the seller. The electronic environments can be used now to exchange any data, any message with anyone, anywhere, and anytime in the world. Forgery, frauds, theft, antisocial activities and other crimes are ever since known to happen in traditional transactions; the electronic transaction is also not untouched by these evils. E-commerce also suffers from cyber crimes and antisocial issues like software piracy, pornography, stealing breaches such as wire tapping, data encryption etc. have impaired this business. Security and privacy are very essential in information business similar to traditional information transfer. The security danger may be to computers and networking systems, where as privacy may be jeopardized due to natural disasters, by theft, or by unauthorized access to the computers. **Virus** may also play havoc and disturb proper functioning of e-business and information system.
Security of transactions is paramount in e-business. The customer must have confidence in this environment, at least at par with that in the traditional business (environments). The technology of e-business should be open (transactions) is taken care of by using clipper chip, keys, antivirus programs, file and data backups, **firewall** and callback systems etc. VoIP presents a likely next likely target because of its growing popularity [1].

2. Electronic/Documentation

With advancement in information technology and communication systems, automation of banking sector has replaced the manual transactions. Installation of computers in banks has improved the working efficiency and provided quicker customer services. Besides day-to-day transactions, notable advancement in payment systems has also taken place in the form of electronic payment system (EPS). Such payments are handled by a machine called ATM (Automatic Teller Machine).
EPS has also changed the method of document handling. For that the magnetic ink character recognition (MICR) technology is widely used now. The electronic payments are being made by MICR cheques using various equipments viz. encoder, reader and sorter. Electronic cash (e-cash) is overwhelmingly used in business transactions. Security and safety to e-cheques and e-cash in transactions are provided by means of digital signature.

Electronic payment systems have also opened new avenues in e-commerce. Electronic data transfer (EDT) and Electronic fund transfer (EFT).are now possible easily and quickly. Such transfers can be accomplished at point of sale (POS) or through banking networks. Uses of credit and debit cards, smart cards have further eased the horizon of e-business.

Electronic clearing services have also undergone tremendous changes. Through SWIFT it has now become possible to interact with member banks throughout the globe.

Various software programs have been developed to assist in digital currency operation and payment systems. Electronic payment in different countries can be made in no time due to availability of conversion software for this purpose. Banking codes, transaction codes, personal identification number (PIN), master card, mondex and chip are upcoming instruments to make EPS more viable.

3. Cyber Crime and Antisocial Issues

Some of the challenges to new technologies in the field of computers, Internet and World Wide Web are computer crimes and antisocial issues. These are on the rise these days and can be in different forms, such as given below.

- Electronic romance
- Electronic pornography
- Software piracy
- Stealing business secrets/documents/data
- Erosion of moral values
- Unauthorized access to a program or information
- Misuse of credit card number
- Defacing of websites
- Impersonation and stealing of personal data
- Internet squatting
- Breach of confidentiality of documents/data

For an e commerce organization the protection of data from loss, damage, misuse, error, or from unauthorized access is of greater concern. In the absence of such protection, the organization will not be able to serve its client effectively. To protect data from loss, the business organizations must keep their proper backups.

The nature of computer crimes may be intentional or unintentional, may be done from a remote place or a nearby location, and can be done by an expert or a common user. The crime may be done for the purpose of financial gains, for stealing a secret, or just for fun. Computer crime done by a professional is against the prestige of the profession [3]. To curtail these crimes, some codes of conduct (ethics) have to be followed. These conducts can be enforced by a regulation or maybe self-binding. Some codes of conduct in this regard are given later in this chapter.

4. Security Issues Related to E-Commerce

The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing [2]. Everyone using a network for sending data or exchange of information assumes that everything that they transfer is secure and intact; and it reaches the desired destination without any harm .this is not always true. Lack of security is a matter of concern and a critical problem when dealing with confidential information, commercial transactions, and research works etching e-commerce transactions where consumers are required to set up an account number and to order the products/services online, at least the following points should be taken care of for security [3].

1. Authentication, to make sure of the client's identity
2. Certify client authentication and access control.

Parties involved in electronic business transactions have their main concern on the following safety issues.

- Reliability of data/information on the web i.e. their genuineness.
- Authenticity and validity of transactions taking place.
- Security communication and exchange of data.
- Authenticity if financial transactions.
- Security of data available on website and servers etc.

When a consumer is shopping on the internet; then in fact he is viewing the information on computer terminal, placing the order and making payment through electronic mode. But, he is not sure whether the shop exists physically or not, and whether he will get the delivery of goods or not, for which payment has been made. Based on the steps and procedures of e-commerce, the rarer a number of transactions where security checks are required these checks are to verify whether

1. The shop for purchasing really exists or not i.e. it is genuine or fake
2. There is guarantee of delivery of goods after making payment or not.
3. The exchange of information is secured, or someone is tampering with it or modifying it for his benefits
4. The delivery made by the seller actually reaches the consumer or not.
5. Information regarding credit card number, address, phone number, email ID, passwords etc, will be kept secret or not.

A better security system will enhance the confidence of consumers at internet and will boost the use of e-commerce. The security systems should also take care of the operational difficulties generally being experienced by the traders. There must be a system to authenticate seller and the buyer to prove their trust, beyond the Password technique. Secure and safe data exchange, protection against any unauthorized access, validity of payment by way of electronic transactions etc must be looked as essential part of e-commerce security.

4.1 Caution against threat to security and measures to check them.

Although the threat to security system cannot be checked to utmost success but it can be minimized by keeping a tight vigil for its complete control. The reason is that the internet is a network of networks, and is open to a very large number of users globally. There are some people who play with the security system, some do experiments by breaking the security barrier to enhance their knowledge and for in depth studies. Some do it just for fun also. The attack on security system is also done to again fraudulently, the data under transmission, or by tapping the information. By keeping a close watch on related operations, the security threat can be minimized to a greater extent, but it probably cannot be eliminated for ever.

The adherence on the systems and procedures for operating and working on the internet minimizes the risks of security failure. Therefore, working on an insecure environment should be avoided. One should be cautious about the viruses also and whenever they are detected, the system should be stopped instantly and a thorough enquiry be made regarding the possible viruses. The authentication of seller and buyer is the base of e-commerce and so proper care must be taken while transferring the information between them.

Any change in behavior of network or computer system should be carefully noticed. For any unusual behavior, it should be checked seriously. It should also be ascertained whether there was some mischief or not. These preventive actions will help in minimizing the damage and will keep the system in normal state.

Some indications are given below which may provide the clues for possible attempts on breaking the security.

- Changes in the disk space.
- Presence of unwanted files in the system.
- Tampering of security file and database, related to security.
- Unusual display of computer system.
- Change in the size of files.

The users are required to be careful on above aspects of security and should keep a watch on the system and behavior of network. It is always advisable to have a proper backup of data in computer, in secondary storage devices like CD, data drive, floppies etc.

5. Types of Security Breaches

E-commerce is prone to several kinds of security breaches. Main among them are the following.

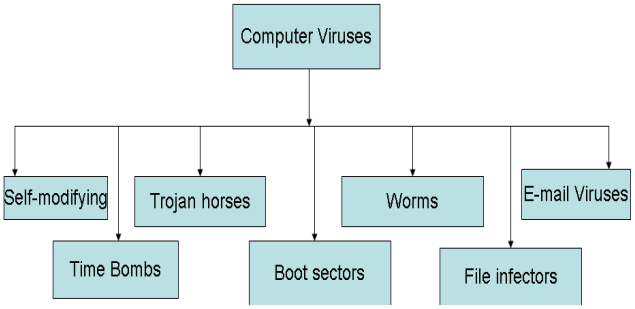
- Virus attack.
- Credit card forgery.
- Data encryption.
- Sabotage in the premises.
- Natural disasters.
- Fire.
- Loss of e-mail privacy.
- Wire tapping of data.
- Theft of hardware/software.
- Unlawful access to files.
- Power line surges.
- Breach to privacy due to electronic fund transfer.

These dangers to security have to be looked after carefully. Their details are discussed in the subsequent sections.

5.1 computer viruses

Unlike biological virus which is living organism, a computer virus is non-living, and unnatural species. The computer virus is a program that is capable of destroying or altering the data stored in a computer system. Once designed, these viruses can pass from one computer to another: over the networks, on floppy disks and modems.

A computer virus can cause immense damage to a large number of computers. It can destroy important documents, research details, and secret data of critical nature. In April 2000, a computer virus 'I love you' caused considerable damage to thousands of computers connected to the internet. Numerous computer viruses are known to exist, and many more are being written each day and every week. Based on the nature of threat and/or destruction they cause, viruses can be classified into various categories. These are



Self-modifying viruses They affect the data file or the program such that each new copy gets slightly altered from the previous one.

Time bombs These viruses enter a computer system, remain there without causing any harm till a certain date or event, on which they become active and destroy the contents of hard drive.

Trojan horses These viruses contain hidden instructions to perform a malicious task and thus to jeopardize the system. They may be in the form of a utility program or as a game; and when run by the user, may erase the data on the hard disk.

Boot sector viruses They get loaded whenever the computer is booted, and make the stored data in the disk inaccessible.

Worms. They affect the systems by taking their (systems) control temporarily. Their effect is to corrupt the data and to cause damage of permanent nature.

File infectors. These viruses are generally hidden on a floppy disk and transfer themselves to any hard disk in whose contact it comes through. Upon inserting another floppy disk into the computer containing the above hard disk, these viruses copy themselves onto that floppy disk. These viruses spread from program to program and it turn ruin codes, data, and directions.

5.2 E-mail viruses. They come through e-mail messages and spread like an epidemic in few hours. In due course they destroy files, data, photos and other documents. They also affect the hard disk of computer ad can stop the working of ATMs also.

Several e-mail viruses are known to exist, a brief account of main among them is given below.

1. Polymorphic virus: It changes the subject of computer and the program codes each time after its transmission. The virus is also named as 'newlove', 'BBS' etc.

2. Love virus: With the subject line of e-message as 'I love you'; this virus destroys 'photons in the photo library', can stop working of ATMs, and destroys other systems of computers.

3. Melisa: It attacked the Microsoft Windows in 1999.

4. Explore Zip: It behaves similar to Melisa virus.

5.3 Wire Tapping and Data Encryption

This kind of security breach may be done by breaking the communication wire and reading the message addressed to someone else. Analog communication (such as done traditionally on telephone) can be easily tapped than a digital communication. To prevent such tapping, use of **clipper chip** is a likely solution. This clip automatically encrypts all the data received or sent over the digital communication lines. **Encryption** of data means translating it into secret code which cannot be *deciphered* without a key.

5.4 E-mail Privacy

Business people (as an individual or as a company) use e-mail to send their messages to the related individuals or firms. These require privacy protection similar to postal mails. E-mail messages are mainly protected by use of secret password. Other method of protection can also be used. These are described later in subsequent articles.

5.5 Credit Card Record Matching

On purchasing an item through e-business with credit card, the chances that the seller will keep track of purchaser's particulars: like addressee, occupation, age, income etc. cannot be ruled out. The seller or the selling company can learn more about the buyer by matching the records and combining facts from the buyer's database such as banking records, payroll records, income tax records etc. Such unauthorized collection of personal data is viewed by many people as an invasion to privacy and can be misused also.

5.6 Electronic Funds Transfer (EFT)

In EFT systems all the transactions related to customers are invariably recorded. These transactions may be in the form of a pay-in-cheque or withdrawal from an automated teller machine (ATM). The transactions are also recorded when the ATM card is used in a petrol station, provision store, or for a refund warrant from a stock market company. Exposure of such transactions can also be viewed as a beach to privacy.

6. Breach Protecting Security Technologies

The problems of security breaches in e-commerce can be handled easily by employing various security technologies. Important among these technologies are the following:

- Virus vaccines (or antivirus programs).
- Use of codes and ciphers.
- Use of sanity checks.
- Employment of public key and digital signatures.
- Using of passwords.
- Establishment of disaster recovery plan.
- Use of callback system.
- Installment of firewall.
- Provision of MS Explorer and internet Protocols.

Besides above, the use of power line surge protectors, uninterrupted power supply, smoke detectors, and physical protection to the system etc. should also be installed as safety measures. We have already described some of these technologies earlier. Some more of them will be discussed now in the following articles.

6.1 Vaccines (or Antivirus Programs)

Analogous to treatment of biological viruses by vaccines (medical drugs) the computer viruses are also treated by computer **vaccines.** These vaccines are in the form of programs; hence they are also known as **antivirus programs**. The virus protection in computers is accomplished by different methodolologies, such as given below:

1. By providing in-built virus protection capabilities in microcomputers,

2. By employing a virus checking programs that run automatically whenever a computer is booted.

3. By screening any download files.

4. By checking the floppy disc for virus, whenever it has been used on another system or contains files from another system.

Amongst these, some antivirus programs are such that they monitor the computer system continuously. In doing so if they notice any unusual activities, they provide either alert or lock the system. Norton antivirus, PC cilin, MacAfee, and Dr. Solomon are some such antivirus programs.

Destroying the Virus by Key -Stroke: According to an expert opinion, the use of key-stroke may be made to nullify the virus effect. For that the following steps should be exercised by the window users.

- Open the control panel and go to Internet option.
  Now go to custom setting and make everything inactive related to Window scripting.

The whole operation takes only a few seconds

6.2 Protecting the data in computers

To protect right of individuals for their personal data such as bank balance, amount received from a sale of property/shares, or a personal buisness details etc; the data in computers have to be protected. The protection is normally desired in the following aspects.

- From theft.
- From sabotage.
- From unlawful access.
- From natural disasters.

For protection against theft and sabotage, the computer rooms have to be kept under strict security. The hardware can be also be fastened with the computer tables. In other cases, various methods such as given below may be adopted.

1. Surge protectors should be used to guard against the surges in power lines.

2. An Uninterruptible Power Supply (UPS) should be used to protect the system for sufficient duration (30 minutes to several hours) if power fails.

3. Smoke detectors and fire extinguishers must be installed for protection against fire.
4. User name and **password** system should be used in the computer system and LAN.
5. Password should be changed frequently and must be out of imagination to others (i.e. obvious words such as date of birth, self name, names of close family members should not be used).
6. Programs may be installed on a separate microcomputer that may be given a password to access these programs.
7. In large organizations, **magnetic access cards** of different security levels should be given to employees serving at different locations (security desired may be more at 1 location and less at the other).
8. To keep employee's movement restricted to a certain zone decided for him, infrared or radio signals emitting badges should be used. These signals can be picked up by sensors and conveyed to central monitoring system so that the location of every individual can be ascertained.
9. Programs and data should be **backed up** regularly by storing them away from the computer system. The backs up may be full or incremental.
10. A disaster recovery plan should be established to meet the unusual situation when a computer is destroyed. This plan should include an alternate computing facility that may be used for emergency processing.

6.3 E-Business network Safety Control

Whereas the sharing of e-business files on network is good facility, it also presents some security problems. It is because these files can be easily accessed from a nearby or remotely located computer (using modems) and thus the company's business data may be stolen. To provide a safeguard against such lapses, several network control methods can be adopted. These methods are given as follows.

1. Use should be made of private account numbers and passwords for the users.
2. A **call back system** should be used for the users so that their identity may be verified by the computer before allowing them to use it.
3. **Firewall** (a software) should be used in LAN's to offer security to data and files.

Protecting the Privacy: Every individual has a right to privacy in his/her activities. It is more so essential incase of e-business. In modern marketing era, the computers are used to help individuals and companies in selling and buying their products. In doing so the use is made of e-mail. Credit card, electronic funds transfer etc. So privacy is desired in all these cases also.

7. Types of Firewalls [3]

Firewall is a means (software) of providing security to documents on the internet. It restricts the flow of data between the 'network of a firm' and the internet. Firewalls are of different types depending upon the level of security provided by them they are classified into following three types

1. packet-filtering firewall
2. circuit-level firewall
3. Application-level firewall.

In each type of firewall, a device (router, computer and switch) is installed between the firm's network and internet.

In packet-filtering type, a router serves as firewall. The router is equipped with data tables and allows the flow of only certain types of message from a location. It provides a single point of security while directing the flow of data traffic.
In circuit level type, a computer is used as firewall instead of a router. The network programmer creates the necessary code for this computer for execution of transaction. Although the circuit- level firewall is better than the packet-filtering firewall, yet it provides single point of security only.
Application-level firewall is most efficient amongst all types since it provides complete security to the firm's internal network. In this system, a security zone is created between the firm's network and the internet. This zone consists of an isolation mechanism (separated from internet by a router) that contains several devices for security screening. To provide security, specific codes are used for each application and they are modified in accordance with the modifications in the application.

References

1. R. Mogull, C. Moore, D.L. Fraley, et. al, “Predicts 2004:Critical Infrastructure Protection,” Gartner Research, January14, 2005.
2. Rhee, M. Y. (2003). Internet Security: Cryptographic Principles,Algorithms and Protocols. Chichester: Wiley. ISBN 0-470-85285-2.
3. "Safety and security on the Internet Challenges and advances in Member States", Based on the findings of the second global survey on eHealth Global Observatory for eHealth series - Volume 4; e-link www.who.int/goe/publications/goe_security_web.pdf

