Excel Journal of Engineering Technology and Management Science
(An International Multidisciplinary Journal)
Vol. I No. 2 January - June 2012 (Online) ISSN 2277-3339

COMPUTER SECURITY

* ***Pritaj.P.Mhaske****, Lecturer, People's Education Society's PES Polytechnic, Aurangabad.*

INTRODUCTION

In Today's Modern world security plays immense vital role in the life of individual. Security means keeping a secret or it implies that information is preserved. It truly said by one of the philosopher that "Three people can keep a secret only if the two of them are dead." This statement is truly said by **Benjamin Franklin –**

First thing keeping the security is not easy a matter of fact, Human tendency is such that when told something in a secret & ask to keep its secret, people are actually quite eager to share that secret with everyone else is often said that to make something public, its should be called Secret and to be told in a hush-hush manner to many people as possible. The word of mouth it automatically spread it.

There are Five generation of computer each generation of computer is characterized by major technology development. They are as follows:

1. First Generation : (1940-1956) : Vacuum Tube
2. Second Generation: (1953-1963): transistor
3. Third Generation :(1964-1971): Integrated Circuit
4. Fourth Generation :(1971- Present): Micro Processor.
5. Fifth Generation : (Present –Beyond): Artificial Intelligence

In the era of second generation of computer i.e. (1950-1960) there was no great deal of Emphasis on security because the system in those days there proprietary or closed. Although the computer exchanges data and information with each other, they form a part of network that was completely under the control of an organization. The protocol used for to computer – Communication in those days were also not known to the general public. Therefore the chances of getting an access to the information being exchange were not very high. That is the important reason that information security was not a major issued in those days. Now the mini computers and micro computers in 1970s and 1980s the issue of computer security started to gain from prominence. However it was not still an item of the highest priority on the agenda of the manager & Technologist.

However the era of computer came in to the existence. An internet is a network of network in which user at any one computer can, if they have permission, get information from any other computer. It was conceived by ADVANCED RESEARCH PROJECT AGENCY (ARPA) of the US GOVERNMENT IN THE YEAR 1996.

NOW the stupendous growth of internet opened up unlimited opportunities for computing. However at the same time it also brought about the plethora of new issues and concerns chief among them being the security information exchanged.

Examples for above:

1. It was no longer safe to send your credit card details over network.

2. A person accessing the connection between sender and the recipient could read the E-mail being exchanged.
3. People would try to login with someone else credential, and use the privileges of that person.

Now there are various new threats and possible attack on information. Therefore it is very important to know how we can make information exchanged secure. Hence the question arises "Why is security required in first place?" Hence we discuss a few real incidents that should prove beyond doubt that security cannot be simply compromised.

Especially these days when serious business and other type of transactions are being conducted over the internet to such a large extent, inadequate or improper security mechanism can bring the whole business down, or play humor with life of people since electronic documents and message are now becoming equivalent to paper document in terms of their legal validity and binding, we examine their various implication in this regards. Hence there is need for security.

NEED FOR SECURITY

First thing, basically computer applications were to handle financial and personal data, the real need of computer security was felt like never before. People realized that data on computer was extremely important aspect of modern life. There are various security holes. First of all an intruder i.e. an intruder means no matter how much secure a system is made there by attacker, who would constantly try to find their way or they try to intrude in to privacy of networks. Intruder can capture the credit details as they travel from the client to the server. If we somehow protect this transit from an intruders attack.

Example for this:

1. One Russian attacker actually managed to intrude in to merchant internet site an obtained 300,000 Credit card from its database. He then attempted extortion by demanding protection money ($100,000) from merchant. Merchant refuse to oblige following this the attacker publish about 25000 Credit card Number on the internet. Some Banks reissued all the credit card at a cost of $ 20/card. Such attacks lead to great losses both in terms an goodwill and finance. Hence therefore if a bank has to replace 300,000 such cards at the rate of $20 the total cost of such attack about 6 million dollars. This problem could have been solved if the merchant had employed proper security measure.
2. In 1999 a Swedish hacker broke in to Microsoft hotmail Web site and created a mirror site. This site allowed to anyone to enter any hotmail users E-mail ID and read her E-mails.

PRINCIPLES OF COMPUTER SECURITY

1. **Confidentiality:** It specifies the only the sender and the intended recipient should be able to access the content of a message confidentially get compromised if an unauthorized person is able to access a message.
2. **Authentication:** Mechanism helps to established proof of identities the authentication process ensures that the origin of electronic message or document is correctly identified.

3. **Integrity:** When contents of message are change after sender send it but before it reaches the intended recipient he says that the integrity of the message is lost.
4. **Non reputation:** Non reputation does not allowed the sender of the message to refute the claim of not sending that message Ex: there are situations where the user send a message later on refuse that she had sent that message for instance user A could sent a fund transfer request to bank B over the internet. After the bank performs the fund transfer as per a instructions, A could claim that she never send the funds transfer instruction. Hence the principles of non-reputation defeats such possibilities denying something having done by it.
5. **Access Control:** Access control specifies and controls who can access what. For instance we should be able to specify that user A can view the record in database, but cannot update them, However user B might be allowed to make updates as well.
6. **Availability:** The principle of availability state that resource should be available to authority parties at all times.

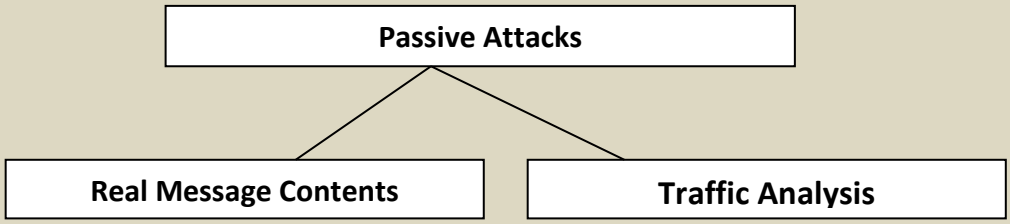
TYPES OF ATTACK

There are two types of attacks:

1. **Passive attacks**
2. **Active attacks**

Passive Attacks: Passive attacks are those where in the attack indulges in cause or monitoring of data transmission. In other words the attacks aim to obtain information that is in transit.

Active Attacks: Unlike passive attacks, the active attacks are based on modification of the original message in some manner or the creation of a false message.



Active Attacks are as follows:

1. **Masquerade:** Masquerade is caused when unauthorized entity pretends to be another entity. User B might be led to believe that a message indeed came from user A.
   A masquerade attack an entity poses as another entity in masquerade attack usually some other forms of active attack are also embedded.
2. **Replay Attack:** In a replay attack a user capture a sequence of events or some data units and resend them. Alteration of message involves some changed to the original message. Transfer $1000 to this account to bank B user C might capture this and changed it to transfer $10000. Note that the beneficiary and the amount have been changed, instead of only one of this could have also cause alteration of the message.
3. **Denial of Service:** An attacks make an to prevent legitimate user from accessing some services which they are eligible for instance an unauthorized user might send to

many logic request to a server using random user IDs and deny other legitimate user from using the network facility.

VIRUS

There are different types of viruses first we will see what is a virus? Virus : In simple term a Virus is a piece of Program code that attacks its self to legitimate program code and runs when the legitimate programs run. In simple words Virus is computer program that attaches itself to another legitimate program and causes damage to the computer system or to the network.

1. **Dormant Phase:** Here the virus is idle. It get activated based on certain action event user typing a certain key.
2. **Propagating phase:** In this phase a virus copies itself and each copy starts creating more copies of self, thus propagating the virus.
3. **Triggering Phase:** A dormant virus moves in to these phase when action/Event for while it was waiting for invitation.
4. **Execution Phase:** This is the actual work of the virus which could be harmless or destructives.

Virus can be classified into following categories:

A. **Parasitic virus:** This a most common form of virus such a virus attacks its self to the executable files and keep replicating. Whenever the infected files is executed. The Virus looks from other executable file to attach itself and spread.
B. **Memory resident virus:** this type of virus attaches itself to an area of the main memory and then infects very executable program i.e. executed.
C. **Boot sector virus:** This type of virus infect the master boot record of the disk.
D. **Stealth virus:** This virus has intelligent built in, which prevent antivirus software program from detecting it.
E. **Polymorphic virus:** Virus that's keeps changing its signature on every execution.
F. **Metamorphic Virus:** In addition changing its signature like a polymorphic virus this type of virus keep rewriting its self every time.

WORM

Worm similar to the concept of virus. Worm is actually different in implantation from its main factor is it replicates its self and make different forms.

Example:

Trojan horse: A Trojan horse is a hidden code like virus, a Trojan horse attempts reveal confidential information to attacker.

ANTIVIRUS

A utility that searches a hard disk for viruses and removes any that are found. Most antivirus programs include an auto update feature that enables the programs to download to profile of new viruses so that it can check for new viruses. As soon as they are discovered.

Generation of Antivirus

1. **First Generation:** these antiviruses s/w program were called as simple scanners, they needed a virus signature to identity a virus.

2. **Second Generation:** these antivirus S/w program did not rely on simple virus signature rather they are used heuristic rules to look possible virus attack.
   For Example, Such program could look for encryption key used by virus to find it, decrypt and remove and clean the code.
3. **Third Generation:** These antivirus s/w program were memory resident, they watch for viruses based on action, rather than their structure. Thus it is not necessary to maintain a large database of virus signature.
4. **Fourth Generation:** These antivirus s/w programs package much technique together they also contain access control feature thus thwarting the attempt of viruses to infect the file.

There is a category of software called as behavior blocking Software, which integrate with the OS of the computer and keeps a watch on virus like behaviour in real time.

Different Antiviruses are as follows:

1. Quick Heal
2. Net protector
3. Norton
4. Antivirus 7

And many more like this are available in the market.

CRYPTOGRAPHY

The art of protecting information by transforming (encrypting) into an unreadable format called cipher text. Only those who possess a secrete a key can decipher the message into plain text. Encrypted message can sometime be broken by crypt analysis also called code breaking although modern cryptography techniques are virtually unbreakable. Cryptography is used to protect E-mail messages, Credit card information and Code data. One of the most popular cryptography systems used on the internet is pretty good privacy and public key system that used two keys, a public key known to everyone and Private Key that only the recipients of message uses.

CONCLUSION

Finally, one thing we conclude is that computer security is not just a condition but has become a necessity, because an a person in America can transit money from person sitting India by wrong methods using modern techniques, due to which factors like cybercrime etc. came into existence. Now for stopping virus and worms- Antivirus are required. Hence we can state that computer security has a great influence in today's world.

REFERENCE

Books:

1. Cryptography and Network Security – Mr.Atul Kahate
2. Cryptography and Network Security Principles and Practices -William Stallings
3. Computer Security - Dieter Gollman.

Web Site:

1. www.google.com
2. www.webopedia.com