Security Issues Facing Computer Users: An Overview

Ms. Yugandhara V. Dhepe
Dept. of Computer Science and Engineering
Prof. Ram Meghe Institute of Technology and Research Badnera, Amravati.
yugadhepe@gmail.com

Prof. S. P. Akarte
Dept. of Computer Science and Engineering
Prof. Ram Meghe Institute of Technology and Research Badnera, Amravati.
s_akarte25@rediffmail.com

Abstract

This paper is a broad overview of several issues pertaining to computer security. There are two types of computer security one is standalone computer security means security of computer when it is not connected with network and second is security of computer when it is connected with network. Using Biometrics methods the computer user can allow only authentication logins. And by using encryption technique the computer users can secure the data in the computer system. With the help of the firewall the computer user can control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. The overall aim of this paper is to discuss here the security issues facing computer user and methods to secure computer system.

Keywords-Computer security, Firewall, Network Security, Viruses and antivirus.

1. INTRODUCTION.

Computer security measures, procedures, and controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction. Over the past 10 years the Internet has become ubiquitous to the average person in the United States. People of all ages use it on a regular basis, and it has become one of the driving forces of the economy. From banking to shopping to communication, it has radically changed the way many people go about their daily lives. The increased availability of broadband connections will allow more people to experience all that the Internet has to offer. [1]

The issue of computer security first arose in the 1970s as individuals began to break into telephone systems. As technology advanced, computer systems became targets as well. The Federal Bureau of Investigation (FBI) made one of its first arrests related to computer hacking in the early 1980s. A group of hackers known as the 414s, named after their area code in Milwaukee, Wisconsin, were indicted for attacking 60 different computer systems including the Los Alamos National Laboratory and the Memorial Sloan-Kettering Cancer Center. [2]

Along with growth in hacking activity came the spread of computer viruses. Three of the most well known viruses-Cascade, Friday the 13th, and Stoned-all originated in 1987. When computer companies like IBM Corp. and Symantec Corp. began researching ways to detect and remove viruses from computers, as well as ways to prevent infection in the first place, virus writers began developing more elusive viruses. By 1991, more than 1,000 viruses had been discovered by computer security experts.

In this paper the section 2 discusses Common Threats to Computer Security in that malicious code, employee sabotage, denial of service (dos) attack, social engineering. The section 3 covers methods to secure computer systems in that computer password, firewalls–hardware and software, antivirus programs, access cards, biometrics, data encryption. The section 4 and 5 discusses the ethical issues and future of computer security.

2. Common Threats to Computer Security

"Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers." The most common computer security threats are i.e. Fraud & Theft, Errors & Omissions, Malicious code, and malicious hackers, Employee Sabotage, Integrity Threat, Denial of

Service (DOS), Disclosure Threat, Social Engineering & Phishing and Memory Space. Some of them are discussed below. [3]

2.1 Malicious Code

It includes worms, viruses, logic bombs, Trojan horses and all the other executable programs/applications used to damage the computer hardware or operating system. These types of code replicates itself in the system, sends undesirable requests to programs and makes the system very slow or even crash the system. Some viruses even delete or corrupt the data like financial statements.

2.2 Employee Sabotage

Some of the employees commonly know about the computers running applications such as financial databases, attendance system etc. of the employer. This type of employee knows what action can be taken to cause damage or sabotage. Some of the examples are as below,

•Damaging Hardware of the employer
•By deleting the office important data
•Crashing the systems containing critical data of employer
• Changing the informative data
• By inserting incorrect data in records

2.3 Denial of Service (DOS) Attack

This type of attack is very common especially when the computer systems are attached with the internet such as servers i.e. email server, web server. A flood of packets is sent to system with fake addresses that low the performance of the system even crashes the system. This type of attack can be done by

• Consuming resources
• Disrupting configuration information
• Disrupting physical network components

2.4 Social Engineering

In this type of attack, the person gathers information about the company or organization by using his social contacts to the employees of that company. The attacker can show himself as a new employee, a repair person or a researcher for this purpose. He can also call to get information from more than one person of the same organization by asking different questions. In phishing attack, the user/attacker sends the emails to persons showing himself an employee of Credit Card Company and in this way he can get information.

3. Methods to Secure Computer Systems

Many different techniques are used to secure the computer from hacking and viruses attack such as Company Security Policy, Physical Location, System Passwords, Centralized Authentication Server, Firewalls, Anti viruses, Encryption Algorithms, Intrusion Detection Systems (IDS), Virtual Private Network (VPN), Finger Prints, Eye recognition, Face Recognition and Voice Recognition. Some of them are discussed below,

3.1 Computer Password

Different types of computer passwords are used to protect the systems from unauthorized access i.e. computer Operating system password and the user login authentication by the central authentication server. In this way the computers can be made secure on the local area network, internet and as well as standalone system.

3.2 Firewalls – Hardware and Software

A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set. A network's firewall builds a bridge between the internal network or computer it protects, upon securing that the other network is secure and trusted, usually an external (inter)network, such as the Internet, that is not assumed to be secure and trusted.

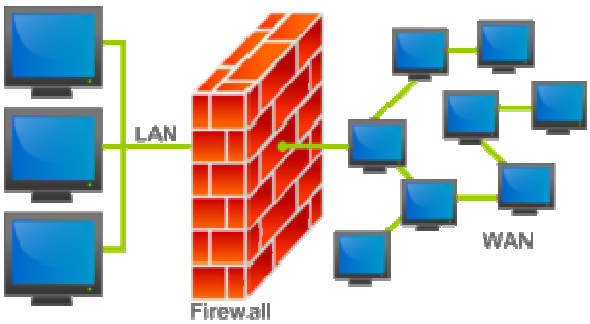

Figure 1: Firewall

There are different types of firewalls depending on where the communication is taking place, where the communication is intercepted and the state that is being traced.

- **Network layer or packet filters**
- **Application-layer**
- **Proxies**
- **Network address translation**

3.3 Antivirus Programs

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. You can help protect your computer against viruses by using antivirus software. To help prevent the most current viruses, you must update your antivirus software regularly. You can set up most types of antivirus software to update automatically.

3.4 Data Encryption

Data encryption is a means of securing data by changing the meaningful text into some code which looks like null and void to others. It's a reasonably easy way to protect information. The user has to remember the key and the software and hardware is secure and user friendly. According to Hoffman there are 900 cryptography hardware and software products on the market. The System administrator normally has access to all files in an information system, therefore the administrator can be a great information security risk, and the risk can be minimized, however, if the classified files are encrypted. [5]

3.4.1 Encryption Algorithms

Such as SSL (Secure Socket Layer), SET (Secure Electronic Transactions) and DES (Data Encryption Standard) are used especially for online banking. All these algorithms encrypt the data for secure communication so that no intruder or hacker can break the security. Message digest is used in DES to encrypt the data or password. It is a 32 byte hash function used as a key.

3.6 Access Cards

Some of the organizations use access cards as identity cards for access the building and as well as for the access of the computers. Different types of access cards are available and some of them are mentioned below.

• Magnetic Stripe Cards (Contains embedded chip which can be programmed.)
• Smart Cards (Contains embedded chip)
• Memory-only Cards (just capable of storing and returning information)
• CPU-Based (Capable of Processing information)
• CPU and crypto-coprocessor–based
• Tokens (these devices can carry information of the user.)

3.7 Biometrics

Authentication is the verification of a user's identity by means of a physical trait or behavioral characteristic that cannot easily be changed. Some of them are discussed below,

- **Eye Recognition**: Two parts of the eye retina and the iris can be scanned but it is slow and inconvenient and may make users uneasy. [6]
- **Fingerprint Recognition**: Fingerprints are unique, readily accessible and require little space for either the reading hardware or data storage.
- **Hand or palm Geometry**: This method relies on devices that measure the length and angles of individual fingers.
- **Voice Recognition**: This is different from speech recognition. The idea is to verify the individual speaker against a stored voice pattern, not to understand what is being said.
- **Facial Recognition**: "Uses distinctive facial features ,including upper outlines of eye sockets, areas around cheekbones, the sides of the mouth and the location of the nose and eyes" [6].

4. Ethical Issues

Most of the people face ethical issues related to computer security such as privacy & integrity, compromised financial data, employee theft, personal privacy, accuracy, property and accessibility. Some of them are discussed below.

4.1 Confidentiality & Privacy

It is the very common ethical issue in computer security. For example:
• Holding the personal information of the employees
• Read emails of the employees
• By tracking the websites visited by the users
• Reading the documents of other users stored on the server
• By looking into the directories of the users

5. Future of Computer Security

Today finger print is the reliable technology used for authentication mainly in high sensitive sectors or companies. The other technologies like voice recognition, face recognition etc are not mature due to some technical problems. In the early future, all these technologies will be built in a single device which will scan all the things including, eye, face, finger, and voice and palm geometry including the height of the person. The person will get access to building and computer by passing from that device.

In the medical field and computer field will become so advance that a chip will be inserted in human body which will contain unique ID number and this person can be able to get access to computer/building and can be monitored from any part of the world by satellite or by any advanced technology at that time. The example of mobile communication best describes the future chip technology. We can go in any part of the world with our mobile set with the unique SIM number provided by our local service provider. With roaming and international roaming, the mobile authentication system can easily trace our current and permanent location/country. On the basis of this technology, in future the person will get access to system by this chip. All the information of this person will be in his chip including bank details, blood group etc. Everything done by him will be logged into his chip and in the central system. If this chip enabled person will do anything wrong like bank fraud, misuse of computer and stealing employer financial data can easily be traced by his chip. Because this chip will log every activity done by he and this chip will not be erasable by himself. A central world organization will issue unique ID's all over the world and data will be stored in a central location.

With the use of artificial intelligence in future, the computers will be so powerful and intelligent that they will grant access to only authorized users. They will monitor all the user activities and in the case of any suspicious activity, they will block that user. The computers themselves will protect from malicious hackers and malicious code i.e. viruses, worms and Trojan horses.

CONCLUSION

This paper present an overview of computer security issues facing computer user. The companies are implementing new and reliable technologies to secure their computer systems from malicious hackers, malicious code and employee sabotage. They are using firewalls and antivirus to protect their systems from viruses, worms and Trojan horses. In order to access the computer, many companies have implemented access card system and biometric system (finger print, voice/face/eye recognition) with the help of these methods the computer user can secure their computer data.

REFERENCES

[1] Michael C. Boeckeler, "Overview of Security Issues Facing Computer Users" March 17, 2004
[2] [2] "Security History", http://ecommerce.hostip.info /pages/249/Computer-Security-History-Computer-Security-Problems.html
[3] "Ethical Issues", http://www.windowsecurity.com /articles/Ethical-Issues-IT-SecurityProfessionals.html
[4] Muhammad Tayyab Ashraf "Computer Security, Forensics and Future Prediction" Canadian Journal on Network and Information Security Vol. 1, No. 6, August 2010
[5] Anjana Bhatnagar "Need Of Information Security In The 21st Century: With Special Emphasis To Computer Security"
[6] Public Domain Biometric Applications: Functionality, Performance, Scalability, Dr T Mansfield, CESG/BWG, Nov 2004.
[7] Concepts and terms' (2005) High Tech Crime Brief www.aic.gov.au/publications/htcb/htcb001.pdf at 12 August 2006.
[8] Richard E. Overill, 'Computer crime – an historical survey'(1998) http://www.kcl.ac.uk/orgs /icsa/Old/crime.html at 20 December 2006.
[9] Michael G. Noblett, Mark M. Pollitt and Lawrence A. Presley, "Recovering and Examining Computer Forensic Evidence"

(2000) Volume 2 Number 4 Forensic Science Communications.

[10] Computer Forensics – Past, Present And Future "Ewa Huebner Derek Bem And Oscar Bem"

[11] Bhavya Daya, "Network Security: History, Importance, and Future University of Florida Department of Electrical and Computer Engineering"

[12] "Wireless Network Protection" Friday, March 14th, 2000

[13] "firewall"http://www.webopedia.com/DidYouKnow/Hardware_Software/2004/firewall_types.asp

[14] "Password"http://en.wikipedia.org/wiki/Passwod