Computer Network Security

Anish P.Bhandari, Anuja K.Raut,Kavita S.Pokarna

Abstract- Computer Network security is the effort to create a secure computing platform, designed so that users or programs cannot perform actions that they are not allowed to perform, but can perform the actions that they are allowed to. The actions in question can be reduced to operations of access, modification and deletion. Computer Network security can be seen as a subfield of security engineering, which looks at broader security issues in addition to network security. However, as more and more people become ``wired'', an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them. It is hoped that the user will have a wider perspective on computer network security in general, and better understand how to prevent, detect, and take counter measures on such threats personally, at home, and in the workplace**.**

———————————— ◆ ————————————

1 Introduction

1.1 Computer Network

A ′′**network**" has been defined as ′′any set of interlinking lines resembling a net, a network of roads | | an interconnected system, a network of alliances." This definition suits our purpose well. A computer network is simply a system of interconnected computers or a system for communication between computers. These networks may be fixed (cabled, permanent) or temporary (as via modems or null modems). Wireless internet generally works over cellular carrier's networks.

Example: Consider an ISO/OSI Reference Model:-
The International Standards Organization *(ISO)* Open Systems Interconnect *(OSI)* Reference Model defines seven layers of communications types, and the interfaces among them. Each layer depends on the services provided by the layer below it, all the way down to the physical network hardware, such as the computer's network interface card, and the wires that connect the cards together. An easy way to look at this is to compare this model with something we use daily: the telephone. In order for you and me to talk when we're out of earshot, we need a device like a telephone. (In the ISO/OSI model, this is at the application layer.) The telephones, of course, are useless unless they have the ability to translate the sound into electronic pulses that can be transferred over wire and back again. (These functions are provided in layers below the application layer.) Finally, we get down to the physical connection: both must be plugged into an outlet that is connected to a switch that's part of the telephone system's network of switches. If I place a call to you, I pick up the receiver, and dial your number. This number specifies which central office to which to send my request, and then which phone from that central office to ring. Once you answer the phone, we begin talking, and our session has begun. Conceptually, computer networks function exactly the same way.

1.3 Types of Computer Networks

There are two types of networks:

1) Client/Server Network
2) Peer to Peer network

1.3.1 Client/Server Network:

Client/server networks consist of two kinds of computer. The clients are usually computer workstations sitting on the desks of employees in an organization. The servers are usually more powerful computers and are held in a central location or locations within an organization. There are several types of servers, for example file servers which store and distribute files and applications, and print servers which control printers.

1.3.2 Peer to Peer Network:

Peer-to-peer networks have workstations connected to each other but do not have servers. Files can be shared between workstations, and a printer connected to one workstation can be accessed by another workstation. Peer-to peer networks are often much simpler to set up than client/server networks. However, they lack some of the advantages normally associated with networks such as centrally managed security and ease of backing up files. Peer-to-peer networks would really only be set up among a few computers within an office or single room.

2. Computer Network Security:-

By the late 1960's, the sharing of computer resources and information, both within a computer and across networks, presented additional security problems. Computer systems with multiple users required operating systems that could keep users from intentionally or inadvertently interfering with each other.

Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.

2.1 Case Study:-

Blackworm Hits 80,000 Computer Systems in INDIA

As many as 80,000 computer system in India and about a million across the world have been estimated hit on Friday 3rd February, 2006 by mass mailing worm Nymex that wrecks computers using the windows operating system.

The virus with aliases such as blackmail, My wife, Grew and its variants has affected 80,000 systems in India.

The virus which would strike on the 3rd of every month had done all the damage it could have done by noon.

The worm infects the system using windows operating system and can corrupt all documents with the file formats like .dmp, .doc, .mdb, .mbe,.pdf, .psd, .ppt, .pps, .rar, .xls and .zip. The worm came to light early December but that time, the number of system infected in India was not confirmed.

Computer Emergence Response Team (CERT) had sent out an advisory to 800 organizations on January 23, 2006 to protect their computer system against the worm.

Top computer security firms have classified the virus as a low threat and provided protection against the worms to the users by January 16, 2006 and none of the customers have reported.

The genuine antivirus software got an upgrade to protect against the attack but in the customer segment the risk of infection was highest as most of the users had pirated software and therefore they got no upgrades.

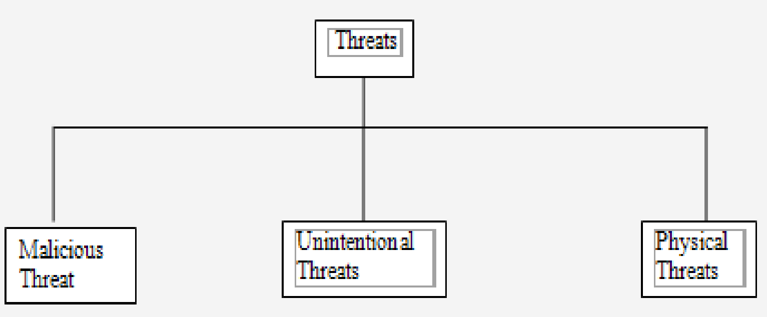
Such types of threats can cause damage to computer network. These threats can be categorized in various ways. Let us see some of the common threats to computer network with their preventions, detection and counter measures.

2.2 Threats to Computer Network:

The nature of computer crime has changed over the years as the technology has changed and the opportunities for crime have changed. Although thrill-seeking adolescent hackers are still common, the field is increasingly dominated by professionals who steal information for sale and disgruntled employees who damage systems or steal information for revenge or profit.

A common view of computer security is that the threat comes from a vast group of malicious hackers "out there." The focus of many computer security efforts is on keeping the outsiders out -- through physical and technical measures such as gates, guards, locks, firewalls, passwords, etc.

Yet, while the threat from outsiders is indeed as great as generally believed, the malicious insider with approved access to the system is an even greater threat! Let us discuss about some threats separately.



Classification of Threats

2.2.1 Malicious Threats:-

Malicious software that attaches itself to other software. "Malicious software" is any software developed for the purpose of doing harm to a computer system. The threat of malicious software can easily be considered as the greatest threat to Internet security. Earlier, viruses were, more or less, the only form of malicious software. Nowadays, the threat has grown to include network-aware worms, Trojans, spyware, adware and so on.

There are many different types of Malicious software:

1. Viruses & Worms:

Spread through e-mail, web pages or networks, these can self replicate and spread to other computers. They can often cause great damage to a computer

2. Trojan Horse*:*

A trojan horse program is a harmful piece of software that is disguised as legitimate software. Trojan horses cannot replicate themselves, in contrast to viruses or worms. A trojan horse can be deliberately attached to otherwise useful software by a programmer, or it can be spread by tricking users into believing that it is useful. To complicate matters, some trojan horses can spread or activate other malicious software, such as viruses. These programs are called droppers.

3. Back Door*:*

A backdoor is a piece of software that allows access to the computer system bypassing the normal authentication procedures. Based on how they work and spread, there are two groups of backdoors. The first group works much like a Trojan, i.e., they are manually inserted into another piece of software, executed via their host software and spread by their host software being installed. The second group works more like a worm in that they get executed as part of the boot process and are usually spread by worms carrying them as their payload.

4. Spyware*:*

Spyware consists of computer software that gathers information about a computer user (such as browsing patterns in the more benign case or credit card numbers in more serious ones) and then transmits this information to an external entity without the knowledge or informed consent of the user.

5. Adware:

Adware or advertising-supported software is any software application in which advertisements are displayed while the program is running. These applications include additional code that displays the ads in pop-up windows or through a bar that appears on a computer screen.

2.2.1.1 Prevention:-

· Every computer that connects to the Internet should have a good virus-scanner and spyware/adware scanning software installed on it and these should be used regularly to scan the system to rid it of malicious software.

· There should be limited connectivity, downloads, write privileges and opportunities to OS files. Use only authorized media for loading data and software

- Enforce mandatory access controls. Viruses generally cannot run unless host application is running
- User cooperation allows Trojan Horses to bypass automated controls hence, User training is best prevention
- Run associated anti-viral software immediately as available

2.2.1.2 Detection:-

- Changes in OS file sizes or date/time stamps

□ Computer is slow starting or slow running

□ Unexpected or frequent system failures

□ Change of system date/time

□ Low computer memory or increased bad blocks on disks Correlate user problem reports to find patterns indicating possible Time Bomb

2.2.1.3 Counter measures:-

- Contain, identify and recover

· Anti-virus scanners: look for known viruses

· Anti-virus monitors - look for virus-related application behaviors

- Attempt to determine source of infection and issue alert
- Contain, identify and recover
- Alert must be issued, not only to other system admins, but to all network users

· Determine source and issue alert

2.2.2 Unintentional Threat:-

In unintentional threat, hardware operates in abnormal way and unintended mode while software behavior is in conflict with intended behavior.

System access for developers is inadvertently left available after software delivery. Inadvertent alteration, manipulation or destruction of programs, data files or immediate loss of data is caused due to abnormal shutdown in this threat.Continuing loss of capability until equipment is repaired. Repeated system failure when re-fed “faulty” data unauthorized system access enables viewing, alteration or destruction of data or software.

2.2.2.1 Prevention:-

- Replication of entire system including all data and recent transactions.
- Enforcement of training policies and separation of programmer/operator duties.

· Limit network and physical access.

· Comprehensive testing procedures and software designed for graceful degradation.

2.2.2.2 Detection:-

- Hardware diagnostic systems
- Software diagnostic tools
- Audit trails of system transactions
- Audit trails of system usage, especially user identification logs

2.2.2.3 Counter Measures:-

- On-site replication of hardware components for quick recovery
- Backup software and robust operating systems facilitate quick recovery
- Close Trap Door or monitor ongoing access to trace back to perpetrator
- Backup copies of software and data

2.2.3 Physical Threats:-

Physical threat of computer is caused due to fire or smoke damage or due to water (including sprinkler) damage. Computers or vital supporting equipment fail due to lack of power. Physical threat may be occur during operations other than war or military action.
In physical threat, immediate loss of data may occur due to abnormal shutdown, even after power returns. Physical destruction of systems and supporting equipment can also be possible.

2.2.3.1 Prevention:-

- Off-site system replication, while costly, provides backup capability
- Dual or separate feeder lines for computers and supporting equipment
- Low profile facilities (no overt disclosure of high-value nature of site)

· OPSEC and low profile to prevent hostile targeting

2.2.3.2 Detection:-

- Network monitoring systems
- Physical intrusion detection devices
- Power level alert monitors
- Water detection devices
- On-site smoke alarms

2.2.3.3 Counter Measures:-

- Hardened sites
- Physical access restrictions and riot contingency policies
- Uninterruptible Power Supplies (UPS)

· Full-scale standby power facilities where economically feasible

· Computer rooms equipped with emergency drainage capabilities

- Halon gas or FM200 fire extinguishers mitigate electrical and water damage

Conclusion:-

The specified data on threats of computer network security has a different idea of what ``security'' is, and what levels of risk are acceptable. The key for building a secure computer network is to *define what security means to your organization*. Once that has been defined, everything that goes on with the computer network can be evaluated with respect to that policy. Projects and systems can then be broken down into their components, and it becomes much simpler to decide whether what is proposed, will conflict with one's computer network security policies and practices.

Many people pay great amounts of lip service to computer network security, but do not want to be bothered with it when it gets in their way. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. Users who find security policies and systems too restrictive will find ways around them. It's important to get their feedback to understand what can be improved, and it's important to let them know *why* what's been done has been, the sorts of risks that are deemed unacceptable, and what has been done to minimize the organization's exposure to them.

Acknowledgement

The making of the paper needed co-operation and guidance of a number of people. I therefore consider it my prime duty to thank all those who had helped us through their venture. It is our immense pleasure to express my gratitude to **Prof. D.N.CHAUDHARY** who provided us constructive and positive feedback during the preparation of this seminar.

We express our sincere thank to the head of department **Dr.D.N.CHAUDHARY** and all other staff members of CSE department for their kind co-operation.

We would like to thank **Dr. A.W.KOLHATKAR**, Principal of our institution for providing necessary facility during the period of working on this report.

We am thankful to our friends and library staff members whose encouragement and suggestion helped me to complete my seminar.

We are also thankful to our parents whose best wishes are always with us.

REFERENCES:-

[1] Akyildiz, I.F., Wang, X. and Wang, W. (2005) 'Wireless mesh networks: a survey', Computer Networks Journal (Elsevier), Vol. 47, No. 4, pp.445–487.

[2] Anton, B., Bullock, B. and Short, J. (2003) 'Best current practices for Wireless Internet Service Provider (WISP) roaming, version 1.0.' Wi-Fi *Alliance*.

[3] Baras, J. and Jiang, T. (2004) 'Cooperative games, phase transitions on graphs and distributed trust in MANET',*Proceedings of the 43rd IEEE Conference on Decision and Control*, pp.93–98.

[4] Finkenzeller K. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification.

[5] Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador J, Ribagorda A. RFID systems: A survey on security threats and proposed solutions. In: 11th IFIP International Conference on Personal Wireless Communications – PWC06, Vol. 4217 of Lecture Notes in Computer Science. Springer-Verlag; 2006. p. 159–70.

[6] RFID Handbook. 2nd ed. J. Wiley & Sons.

[7] Phillips T, Karygiannis T, Huhn R. Security standards for the RFID market. IEEE Security & Privacy (November/December 2005); 85–9.

[8] RFID Handbook. 2nd ed. J. Wiley & Sons.

[9] RFID Handbook. 2nd ed. J. Wiley & Sons.

[10] Phillips T, Karygiannis T, Huhn R. Security standards for the RFID market. IEEE Security & Privacy (November/December 2005); 85–9.

[11] EPCglobal. www.epcglobalinc.org/, June 2005.

[12] Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador J, Ribagorda A. RFID systems: a survey on security threats and proposed solutions. In: 11th IFIP International Conference on Personal Wireless Communications – PWC06, Vol. 4217 of Lecture Notes in Computer Science. Springer-Verlag; 2006.p. 159–70.

[13] Phillips T, Karygiannis T, Huhn R. Security standards for the RFID market. IEEE Security & Privacy 2005;85–9.

[14] EPCglobal Tag Data Standards. Version 1.3.

[15] EPCglobal. www.epcglobalinc.org/, June 2005.

[16] Guidelines for Securing Radio Frequency Identification (RFID) Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800–98.

[17] Thompson DR, Chaudhry N, Thompson CW. RFID Security Threat Model.

[18] Weis S, Sarma S, Rivest R, Engels D. Security and privacy aspects of low-cost radio frequency identificationsystems. In: Stephan W, Hutter D, Muller G, Ullmann M, editors. International Conference on Security in Pervasive computing-SPC 2003, vol. 2802. Springer-Verlag; 2003. p. 454–69.

[19] Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador J, Ribagorda A. RFID systems: a survey on security threats and proposed solutions. In: 11th IFIP International Conference on Personal Wireless Communications – PWC06, Vol. 4217 of Lecture Notes in Computer Science. Springer-Verlag; 2006. p. 159–70.

[20] Haehnel D, Burgard W, Fox D, Fishkin K, Philipose M. Mapping and localization with WID technology, International Conference on Robotics & Automation 2004.

[21] Thompson DR, Chaudhry N, Thompson CW. RFID Security Threat Model.

[22] Thompson DR, Chaudhry N, Thompson CW. RFID Security Threat Model.

[23] Juels A, Rivest RL, Syzdlo M. The blocker tag: selective blocking of RFID tags for consumer privacy. In: Atluri V, editor. 8th ACM Conference on Computer and Communications Security. 2003. p. 103–11.

[24] Juels A, Rivest RL, Syzdlo M. The blocker tag: selective blocking of RFID tags for consumer privacy. In: Atluri V, editor. 8th ACM Conference on Computer and Communications Security. 2003. p. 103–11.

[25] Thompson DR, Chaudhry N, Thompson CW. RFID Security Threat Model.

[26] Thompson DR, Chaudhry N, Thompson CW. RFID Security Threat Model.

[27] Thompson DR, Chaudhry N, Thompson CW. RFID Security Threat Model.