Problems & Laws in Computer security

Mrs. S. S. Bhavsar

Lecturer, Computer engineering Department, V.P.M's Polytechnic, Thane, Maharashtra, India

---****---

Abstract- *Computer security is a branch of information security applied to both theoretical and actual computer systems. Computer security is a branch of computer science that addresses enforcement of 'secure' behaviour on the operation of computers. The definition of 'secure' varies by application, and is typically defined implicitly or explicitly by a security policy that addresses Confidentiality, Integrity and Availability of electronic information that is processed by or stored on computer systems.*

Key words: *Computer security, threats, attacks, security basics, Cyber laws*

1. COMPUTER SECURITY:

"Generic name for collection of tools designed to protect the data of computer system or network and to prevent hackers is called as COMPUTER SECURITY."

1.1 Need for Security:

To protect our electronic data from Disclosure, Change or Destruction of unauthorized individuals, we need computer security.

1.2 Security Basic [1]

According to the definition of computer security, there are three key objectives of computer security:

- Confidentiality
- Integrity
- Availability
- Authentication
- Accountability
- Non-repudiation

2. RISK AND THREAT ANALYSIS

Risk = Attacks x Threats x Vulnerability

- **Attacks:** Attacks are attempts by unauthorised person or individual to access or modify the information of user's computer system or network.
- **Threats:** Threat is set of things which have potential to cause loss or harm to computer system and network.
- **Vulnerability:** Vulnerability is weakness in computer system and network.

2.1 Threat to Security

- Virus
- Worms
- Intruders
- Insiders
- Criminal Organization
- Information Warfare
- Avenue of Attack

Virus
Spyware
Computer Threats
Trojan
Malware
Worm

2.2 Attacks:

- DOS Attack
- Man in Middle Attack
- Sniffing Attack
- Spoofing Attack
- Backdoors and Trapdoors
- Replay Attack
- TCP/IP Hacking
- Encryption Attack

3. METHODS OF ATTACK

3.1 Phone attacks

A preacher is a person who takes advantage of the telecommunications system to make free lone-distance telephone calls, listen to private conversations, access internal systems, or hack into other systems via the system broken into. Preachers are familiar with telephone switches, networks, and other equipment, and often have manuals from the manufacturers of telecom equipment that describe exactly how to operate and repair that equipment. Experienced preachers can manipulate telephone billing, access codes, and call routing.

Preachers can make free long-distance phone calls by gaining "dial-in / dial out" capabilities. For example, a preacher calls a number in your organization, and then asks to be transferred back to the operator. He then poses as an important person within the company and asks for an outside line. His call is now looped through your company, and you pay the bill. Attacks on other systems may be perpetrated in this way. Worse, the targets of the attack may think your company is responsible.

Hackers and preachers even pose as service technicians to gain access to phone closets and PBX systems, where they reprogram the systems, install bugs, or set up circuits that can be accessed late and used to attack your company or other companies.

3.2 Hackers user accounts and passwords attack

An attacker's first priority is to obtain user account names and passwords since this provides easy access to a system. Once inside, the hacker will find away to elevate his privileges. The attacker can obtain a list of user account names from a number of likely sources. For example, the company e-mail system might provide such lists. In high-security environments, make sure these lists are not readily available. Internal users will usually have easy to access to account names. Once a user account list is obtained, the hacker will try to determine which account will give the most access if broken into .the pc support staff may inadvertently provide this information in the form of list of uses to contact in case of problems. Once a hacker obtains alginate user account name, cracking the password is the next step. Hackers take advantage of common passwords: if they know the user of an account, they may try various combinations of the user's kids and pets' names. Many people use the same password to log on to other systems, such as ATM machines. A co-workers/hacker could obtain this password by watching you at the bank machine with a part of binoculars (yes, it's done). A good reason to choose an obscure password is to make it difficult for people with good eyes to follow your keystrokes as you type it.

If a hacker obtains a user account name, but not a password, he can try brute force methods of breaking into the account. A program is set up to try thousands or millions of different passwords until the account opens. This method is ineffectively if logon restrictions that limit the number of attempted.

Logons Are Set Exhaustion attacks and dictionary attacks are methods for cracking password files and other encrypted information .in an exhaustion attack thousands of password combinations are used until a guessed. In a dictionary attack, a complete dictionary of common passwords in multiple in languages is tried until a password is guessed. Hackers often know the manufacture's default passwords to equipment like routers and depend on the fact that the passwords are not changed.

3.3 Electronic eavesdropping and cable sniffing

A packet snifter is a device or software that can read transmitted packets. Packet sniffing is a passive eves dropping technique that is hard to detect. The packet-sniffing devices may be installed on internal or external networks. Although packet sniffing an internet transition line is not necessarily informative, sniffing a cable that runs into your facilities who are armed with packet snifters, or from hackers who have penetrated your building and planted listening devices.

3.4 .Viruses and Trojan horses

Viruses are small programs that mimic the activities of real-life viruses. They get into computer systems by being copied from contained disks or downloaded from online services by unsuspecting users. Once a system is contaminated, the virus executes some immediate action, or waits until a specified time or for a specific command executed by the user. Viruses may display harmless messages or destroy the information stored on entire hard disks. A Trojan horse is similar to a virus, but contaminates a system by posing as some other type of program.

Virus are especially dangerous on networks because once they contaminate one system, they may spread to systems throughout the entire network. The biggest threat is that unsuspecting employees will pick up virus through normal business transactions spread them throughout an organization.

Virus contamination comes from a number of sources:

- Library computers or company kiosk computers that many different people use
- Service technicians who use disk-based utilities to check computers
- Computers infected by malicious users or by disgruntled employees who want to get with the company or another employee. Yes, even packages of off-the –self-software.

In fact, viruses were available for sale in a recent magazine advertisement for the purpose of testing your anti-virus software! Anyone not sure how to get a virus can now just buy one in order to infect someone else's system.

Viruses are created by authors who are fascinated by how quickly their virus may spread through computer systems. Terrorists and industrial spies create viruses that cause damage in order to seek revenge on an opponent or to viruses that cause damage in order to seek revenge on opponent or tom damage the operations of a competitor. Some viruses are intended targets.

3.5 Natural Threats

Obviously, not all threats to the integrity of your network come from people. Power surges, failing components, and other problems may bring down systems and cost your organization thousands or millions of dollars in down time. In some cases, continuous access to information is critical to the operation of the entire business. The following list covers most major natural threats:

- Electrical power may be lost during storms or for other reasons. Backup power supplies are essential.
- Hardware failures can cause loss of data availability. Redundant systems and backup are imperative.
- Fires, floods earthquakes, and other disasters require backup systems and backup are imperative.

In any of these situations, communication lines that are essential to the operation of your company may be cut. You need to establish alternate lines or backup methods to keep system online in emergencies.[4]

4. CYBER SAFETY

The internet is easy, convenient and fun. But all that easy convenience can be risky, and some of the risks can have serious, lasting outcomes.

Personal photos can end up being public jokes, arguments can turn into fully blown, fully documented flame wars and private details can be used against you - illegally or even *legally*.

These kinds of things can happen to anybody, which is why it's important to do your best to stay safe online.

4.1 IT Act and Cyber Law

CYBER CRIME is nothing but where the computer used as an object or subject of crime.

Cyber Laws are contained in the IT Law.

The Acts aims to provide for the legal infrastructure for e-commerce in India.

The cyber laws have major impact for e-business and the new economy in India.

In India, IT ACT 2000 & IT ACT 2008 are there.

- According to cyber laws, Information technology is the important law & it had passed in Indian parliament in year 2000.
- Due to misuse of internet & increase of cyber crime, the govt. of India made a act for safeguarding the internet users.
- The main objectives & scope of act are as follows:

1. To provide legal recognition to the transaction that can be done by electronic way or by using internet.
2. To provide legal recognition to digital signature used in transaction.
3. To provide facilities like filling of document online relating to admission or registration.
4. To provide a facility to any company that they can store their data in electronic storage.
5. To provide privacy of internet user by preventing the computer related crimes.
6. To provide legal recognition for bankers & other companies to keep accounts in electronic form.[2]

4.2 IT ACT 2008:

- It is the information technology amendment Act, 2008 also known as ITA-2008.
- It is a considerable addition to the previous law i.e. ITA-2000 and is administered by the Indian Computer Emergency Response Team (CERT-In) in year 2008.
- Basically, the Act was developed for IT industries, to control e-commerce, to provide e-governance facility & stop cybercrime attacks.
- Following are the characteristics of IT Act 2008:

1. This Act provides legal recognition for the transaction i.e. Electronic Data Interchange (EDI) & other electronic communications. Electronic commerce is the alternative to paper based methods of communication to store information.
2. This Act also gives facilities for electronic filling of information with the Government agencies & further changes the Indian Penal Code-Indian Evidence Act 1872.
3. The general Assembly of the United Nations by resolution A/RES/51/162, dated 30 Jan 1997 has adopted the model law on electronic Commerce on International Trade Law.
4. This recommends that all states give favorable consideration to the above said model law when they enact or revise their laws, in term of need for uniformity of the law applicable to alternative to paper-based methods of communication and storage of information.
5. It is considered necessary to give efforts to the said resolution & to promote efficient delivery of Government services by means of reliable electronic records.[3]

5. CONCLUSION

Hackers and many algorithms are there to break passwords and much valuable information, which leads to a great loss. Hence network security provides the remedy by many ways. Hence much more advanced security measures would be more helpful. So always that should be an eye on network security as it is much and more important.

REFERENCES

1. Principles of Computer Security
Security + and Beyond Wm. Arthur Conkin Author:
Dwayne Williams
Gregory B. White Roger
L. Davis Chuck Cothren
2.http://www.tifrh.res.in/tcis/events/facilities/IT_act_2008.pdf
3.http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf
4.http://computernetworkingnotes.com/network-security-access-lists-standards-and-extended/types-of-attack.html