Network Security & Privacy

What are the reasons for security breaches?

Network attacks are often caused by direct or indirect **interaction of humans.**

If someone can gain enough information and holds the necessary computing skills, he/she can compromise a company's network security somewhat easily. Because network security is mitigated by humans, it is also often susceptible to human mistakes.

What are the reasons for security breaches?

There are many situations in which employees themselves pose the biggest threat to enterprises. Many times, employees will **unintentionally install piracy software** that is infected with viruses, worms or trojans.

Users may **forget to secure their workstations**, leaving them open as an easy target to potential attackers.

Users may **give sensitive information to outsiders**, or even play a role in an important part of an attack. This is why a security policy should include internal and external threats.

What are the reasons for security breaches?

By gaining **physical access to network devices**, a user can extract important information from the company’s servers or storage devices.

Security holes:

- Operating Systems,
- Network devices
- TCP/ICP protocols can be used by the hacker to gain access to network resources.

How to secure the network systems?

It is important to **update device's firmware**, install the latest OS security updates and change the default settings.

Every company should implement a **security policy** where potential vulnerabilities are addressed and treated.

Types of Network Security Attacks

I. Unstructured: attacks made by unskilled hackers. Individuals behind these attacks use hacking tools available on the Internet and are often not aware of the environment they are attacking.

These threats should not be neglected because they can expose precious information to malicious users.

Types of Network Security Attacks

II. Structured attacks made by individuals who possess advanced computing skills. Such hackers are experts in exploiting system vulnerabilities.

By gaining enough information about a company's network, these individuals can create custom hacking tools to breach network security.

Most structured attacks are done by individuals with good programming skills and a good understanding of operating systems, networking and so on.

Types of Network Security Attacks

III. Social engineering : Malicious users take advantage of human's credibility and often gain important information directly from their victims. They often call or send fraudulent emails to their victims pretending to be some other person entirely.

"Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes indirectly, money) by masquerading as a trustworthy entity in an electronic communication". Entire sites are known to be duplicated by hackers in an attempt to steal precious information from users.

Types of Network Security Attacks

Password attacks – These attacks are based on **cracking user or equipment passwords**. They are one of the most feared network attacks because once a user is compromised, the whole **network can be damaged**, especially if we are talking about a domain user or network administrator.

Dictionary attacks use patterns to guess passwords in multiple attempts. Critical information can be gained by using a compromised username. This is one of the main reasons companies **use strong passwords** that are changed frequently.

Types of Network Security Attacks

Exploit attacks – These are usually made by individuals who possess strong computing skills and can take advantage of **software bugs** or **misconfigurations.**

By having enough information of a specific software, hackers can "exploit" a particular problem and use it to gain access to private data.

Types of Network Security Threats

Logic attacks- A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

like **backdoors**, to **security lapses in code**. The aim is to break into the system, either to crash it or to grant access to an unauthorized individual.

Types of Network Security Attacks

Eavesdropping is one of the common types of attacks. A malicious user can **gain critical information** from **"listening" to network traffic**. Because most communications are sent unencrypted, there are many cases in which traffic is susceptible to interception. The traffic can be analyzed using sniffing tools (also known as snooping) to read information as it is sent into the network.

Wireless networks are more susceptible to interception than wired ones.

Eavesdropping can be prevented by using encryption algorithms.

Types of Network Security Attacks

Compromised-Key attack – by obtaining the **private key** of a sender, an attacker can decipher secured network traffic. This kind of attack is often hard to be carried out successfully because it requires good computing resources and skills.

Man-in-the-Middle attack – as the name implies, this attack is based on **intercepting** and **modifying** information between two transmitting nodes. A hacker can modify network routes to redirect traffic to its machine before it is carried out to the destination.

Types of Network Security Attacks

IP address spoofing – In this scenario hackers use spoofed IPs to impersonate a legitimate machine. The attacker can then modify packets making them look like legitimate traffic to the receiving network device.

Application-layer attacks – these attacks are based on **cracking applications** that run on servers or workstations. These types of attacks are common because there are many different applications that run on machines and are susceptible to attacks. Hackers use viruses, Trojans and worms to infect devices and gain important information.

Types of Network Security Threats

Resource attacks, aim to overwhelm network resources to the point of collapse. This is called Denial of Services.

The idea of resource attacks into force the system to crash, and therefore become vulnerable. These attacks are carried out in a number of ways; most easily by flooding a server with more service requests than it can handle.

Some resource attacks involve the installation of malware on the network, causing it to become vulnerable.

Denial of Service

A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.

In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

Types of Network Security Attacks

DoS and DDoS attacks (Denial of Service and Distributed Denial of Service attacks)– These attacks take advantage of network traffic to create abnormal behavior to network services or applications. Servers are often targeted and flooded with data until they become unreachable.

Core network equipment can be blocked and thus prevent normal traffic from flowing into the network.

DoS vs DDoS (simple comparison)

Attack Type	Description	Example
DoS	Attack from **one source**	One attacker floods a server with requests
DDoS	Attack from **many distributed sources**	Thousands of infected devices attack simultaneously

Email bombing

Some attackers also act on an another kind of DoS attack – **Email bombing** in which a lot of spam emails are generated and flooded into one's Inbox so that any further request to the mail server are debarred. This can happen widely, even on the email account provided to you by your employers, not to mention the public mail services like *Yahoo, Outlook etc*. You can even get deprived of receiving any further legitimate emails as your allotted storage quota will be filled up. With a great deal of variety in their ambitions, the motivation of attackers may range from 'just-for-fun' to financial clinch to revenge.

Backdoors

The system administrators may have back doors installed in their systems. These back doors can have two common forms of either an extra user account with system administrator privileges or a hidden back door to access the system by running a specific command at system level.

This is particularly troublesome for the organization, since it means that the system administrator would have access even if his job was terminated. Also if by chance a hacker found this backdoor then he also would have complete access to the company proprietary information.

Time Bomb

An even worse nightmare for a manager is if one of his system administrators installs a time bomb in the system. These programs require some steady input in order for them to stay dormant. This input can usually be of the form of the system administrator logging on to the network. Therefore the time bomb would activate only in the case that he/she didn't log on to the network for say a whole month. Once activated this time bomb is unstoppable and would result in at least major disruption of computer services and in more drastic scenarios could also end in complete system obliteration

Stealth Backdoors

Once again there are plenty of tools available over the Internet to do just this. The system administrator can use these tools to actually install a stealth back door that unlike a regular account does not show up in regular audits. Such back doors even allow remote connections and since the account has root privileges, the system administrator, once remotely connected to the system, can run/install anything on the machine and he/she has the potential to do a lot of harm

Countermeasure

Special logging software should be used and singular attention should be given to any remote connections that are established out of the ordinary.

All software installation records should also be kept safely for auditing and if possible the main system should be configured to require dual authentication for both installation and uninstallation.

Another easy technique for the managers is to ask different system administrators to perform an audit each time .

In the case where there is only one system administrator then the responsible company should look into getting an outside independent auditor to carry out a surprise audit on their system looking specifically for such backdoors and Trojans and time bombs.

Computer Fraud

Computer Fraud is a deception for personal gain in online business transactions by assuming a false online identity or by altering or misrepresenting data.

Cyberterrorism and Information Warfare

Cyberterrorism is defined as the execution of "politically motivated hacking operations intended to cause grave harm, that is, resulting in either loss of life or severe economic loss, or both".

Hacktivism, which are hacking operations against an internet site or server with the intent to disrupt normal operations but without the intent to cause serious damage.

Cybertrespass

Cybertrespass is defined as the use of information technology to gain unauthorized access to computer systems or password-protected websites, and **cyber-vandalism**, which is the use of information technology to unleash programs that disrupt the operations of computer networks or corrupt data.

Cyber-piracy

Cyber-piracy, also called software piracy, is the use of information technology to reproduce copies of proprietary software or information or to distribute such data across a computer network.

Cyber-piracy is much more widespread than cyber-vandalism or cybertrespass, because it does not require extensive computer skills and many computer users find it morally permissible to make copies of copyrighted software and data.

Cyber-piracy involves breaches in computer security when it includes the cracking of copyright protections.

Recommendations for a security culture

There are several recommendations that can be applied towards the build-up of a sound security culture in any organization.

Self-Policing:

- It is crucial that system administrators should not consider themselves above the law and should always practice what they preach for example copyright laws.

Recommendations for a security culture

Password Security:

Use strong passwords for all account types.

Do not use default account names, and rename standard accounts such as the administrator's account and the anonymous Internet user account used by many Web applications.

Apply lockout policies to end-user accounts to limit the number of retry attempts that can be used to guess the password.

Install software that manages logins on every system. Every time a user logs on to the network, this software should message the user and indicate the time and date for the last successful login.

Recommendations for a security culture

Web site administrators can minimize the danger that their IP addresses will be spoofed by implementing one-time passwords.

Two-step verification for logging attempt.

Audit failed logins for patterns of password hacking attempts.

Recommendations for a security culture

Security Software:

Deploy an **antivirus** program and **firewall** into your network if not already done. This helps in restricting the bandwidth usage to authenticated users only.

Audits for System Administrators:

Special logging software should be used and singular attention should be given to any remote connections that are established out of the ordinary.

Surprise audits of the system administrators' laptops or desktops should be part of company policy and tradition. Each and every organization should uphold copyright and licensing laws towards all of their employees specially the system administrators.

Recommendations for a security culture

Smart Cards :

- Smart cards have built in memory cards (that cannot be easily hacked with current technology) that can hold digital certificates, encryption private keys and the user's unique personal identification number etc. By utilizing smart card logins the organizations can safeguard the user computer from any snooping by a system administrator since having the PIN of the user is not enough for the system administrators to access the user's computer, the smart card itself is needed as well.

Recommendations for a security culture

Biometrics:

- Biometrics is another technology using which only the individual user has access to his/her computer. So far biometrics include voice, finger and hand printing and retina pattern recognition. Since these characteristics are unique for the individual, the private data and resources are once again safeguarded from any unauthorized access or intrusion. Of course the biometric technology can be combined with the smart cards in order to further secure the authentication process.

Recommendations for a security culture

- **Ethical behaviour**: Companies should try to hire individuals who have a well-rounded personality and who actually enjoy following, enforcing and improving rules and policies and who have at least graduated from an accredited university.
- **Zero Tolerance:** System administrators should be made aware that the illegal behaviour of employees, regardless of how minor it is, would not be acceptable. These actions would be immediately reported to appropriate authorities and exacting actions would be taken against any one who is found to be the perpetrator beyond any doubt.

Recommendations for a security culture

- **Resources:** If the system administrators are over-worked then there is the possibility of them missing out on finer details that a hacker may not overlook. A possible answer to this can be as simple as hiring more system administrators in case the work is exceeding all projections.
  - the system administrators will have more help and more time to really improve security policies in the company
  - Task like revising the firewall's current rule base requires a calm and worry free mind
  - more than one system administrator has the additional advantage of implementing checks and balances within the IT department.