**COMPUTER AND NETWORK SECURITY?**

Network Security is the process through which a network is secured against internal and external threats of various forms.

Computer network and security encompasses the technologies, policies, and practices used to protect computer networks and the data they transmit and store from unauthorized access, misuse, modification, or disruption. It's a critical aspect of cybersecurity, aiming to safeguard the confidentiality, integrity, and availability of information and resources within a network.

**GOALS OF NETWORK SECURITY**

1. **Confidentiality:** This term covers two related concepts:
2. Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
3. Privacy: Assures that individual’s control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
4. **Integrity:** This term covers two related concepts:
5. Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
6. System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
7. **Availability:** Assures that systems work promptly and service is not denied to authorized users.
8. **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
9. **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis

Generally, the ultimate goal of implementing security on the network is achieved by following a series of steps and these steps are:

1. Identify what you are trying to protect.
2. Determine what you are trying to protect it from.
3. Determine how likely the threat are.
4. Implement measures that protect your assets in a cost-effective manner.
5. Review the process continuously and make improvements each time you find a weakness.

**EXAMPLES OF SECURITY VIOLATIONS**

1. User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.

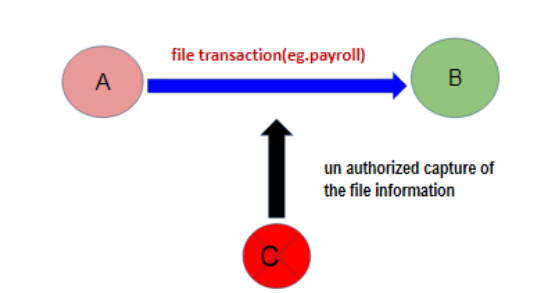


Fig 1: Example 1

1. A network manager, D, transmits a message to a computer, E, under its management. The message instructs computer E to update an authorization file to include the identities of a number of new users who are to be given access to that computer. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E, which accepts the message as coming from manager D and updates its authorization file accordingly.

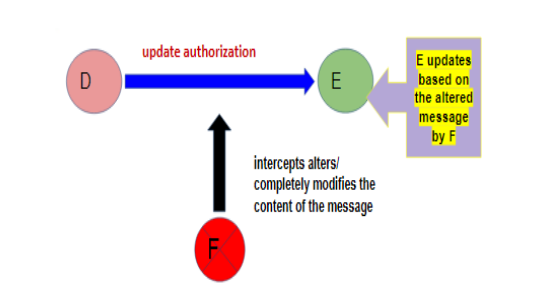


Fig 2: Example 2

1. Rather than intercept a message, user F constructs its own message with the desired entries and transmits that message to E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.

**SOME KEY REASONS WHY WE NEED TO KEEP OUR NETWORK SECURE**

1. **Protect Sensitive Data:** Businesses store sensitive customer, employee, and proprietary data. A secure network helps prevent unauthorized access, leaks, and identity theft.
2. **Prevent Financial Loss:** Cyberattacks can lead to direct financial theft, fraud, or the cost of responding to breaches and downtime, all of which can be very expensive.
3. **Maintain Business Continuity:** Security breaches can disrupt operations. Keeping the network secure helps ensure systems stay up and running without interruptions.
4. **Preserve Company Reputation:** A data breach or cyberattack can severely damage a company’s trustworthiness and brand image, potentially leading to loss of customers.
5. **Prevent Unauthorized Access:** A secure network ensures that only authorized users can access internal systems and information, keeping hackers and insiders in check.
6. **Protect Intellectual Property:** Businesses often hold valuable intellectual property, like designs, software, or trade secrets. Network security helps safeguard these assets.
7. **Avoid Ransomware and Malware**: Without strong network security, companies are vulnerable to malware that can lock systems or steal data until a ransom is paid.
8. **Support Remote Work Safely:** With more remote and hybrid work setups, securing connections to the company’s network is more critical than ever.
9. **Mitigate Insider Threats:** Not all threats come from the outside. Network security also helps detect and reduce risks from malicious or careless insiders.

**WHO IS A NETWORK ADMINISTRATOR & FUNCTIONS OF A NETWORK ADMINISTRATOR?**

A network administrator is a person responsible for managing, maintaining, and securing a computer network within an organization. This includes tasks like:

* Setting up networks (e.g., LAN, WAN, intranet)
* Installing and configuring network hardware like routers, switches, firewalls
* Monitoring network performance and fixing issues when something goes wrong
* Ensuring network security by managing firewalls, VPNs, and access controls
* Managing user access and permissions
* Backing up data and preparing disaster recovery plans

Basically, they're the go-to person to keep a company's internet, internal systems, and connections running smoothly and securely.

**COMPUTER NETWORK SECURITY CHALLENGES AND SOLUTIONS**

Computer network security faces challenges from evolving threats, human errors, and a skills gap, requiring proactive measures like robust security protocols, user education, and continuous monitoring to mitigate risks and maintain a secure environment.

**Challenges:**

1. **Evolving Cyber Threats:** Cybercriminals constantly develop new techniques, making it difficult to stay ahead of the curve.
2. **Human Error:** Phishing scams and social engineering tactics exploit human vulnerabilities, leading to breaches.
3. **Lack of Security Awareness:** Insufficient knowledge about security risks and best practices among users can lead to unintentional compromises.
4. **Skills Gap:** A shortage of qualified cybersecurity professionals makes it difficult to fill critical roles and maintain security.
5. **Third-Party Risks:** Outsourcing tasks to third parties can introduce vulnerabilities if their security practices are inadequate.
6. **Data Security Risks and Vulnerabilities:** Gaps in endpoint security, poor access controls, and limited cybersecurity awareness among employees increase the risk of breaches.
7. **Network Security Vulnerabilities:** Weak points in physical devices or software present opportunities for cyber attackers.
8. **Ransomware:** Ransomware attacks can disrupt operations and lead to significant financial losses.
9. **DDoS Attacks:** Distributed Denial of Service (DDoS) attacks can overwhelm networks and disrupt services.
10. **Firewall Misconfigurations:** Improperly configured firewalls can create vulnerabilities and allow unauthorized access.
11. **DNS Problems:** Compromised Domain Name System (DNS) infrastructure can lead to downtime and data loss.
12. **Slow Internet Connection:** Slow internet can lead to vulnerabilities such as delayed software updates and patch installations.
13. **Hardware Failures:** Hardware failures can disrupt network connectivity and lead to data loss.

**Solutions:**

1. **Implement Robust Security Protocols:** Enforce strong passwords, multi-factor authentication, and regular security audits.
2. **Educate Users:** Conduct regular security awareness training to help users identify and avoid phishing attempts and other threats.
3. **Invest in Cybersecurity Skills:** Provide training and development opportunities for IT staff to enhance their cybersecurity skills.
4. **Continuously Monitor Networks:** Implement intrusion detection and prevention systems to identify and respond to threats in real-time.
5. **Patch and Update Regularly:** Ensure that all software and hardware are up-to-date with the latest security patches.
6. **Use Strong Antivirus and Antimalware Software:** Install and maintain up-to-date antivirus and antimalware software on all devices.
7. **Implement Access Controls:** Restrict access to sensitive data and systems based on the principle of least privilege.
8. **Back Up Data Regularly:** Regularly back up critical data to prevent data loss in the event of a security incident.
9. **Stay Informed:** Keep abreast of the latest cybersecurity threats and best practices.
10. **Consider Third-Party Security Assessments:** Conduct regular security assessments of third-party vendors and partners.
11. **Implement a layered security approach:** Combine multiple security technologies and controls to create a robust defense.
12. **Focus on Physical Security:** Secure physical access to network infrastructure and devices.
13. **Address Network Connectivity Issues:** Ensure reliable and high-speed internet connections to minimize vulnerabilities.
14. **Optimize Firewall Configurations:** Ensure firewalls are properly configured and regularly updated.
15. **Implement DNS Security Measures:** Use DNSSEC and other DNS security measures to protect against DNS-related attacks.

**Firewall:** a firewall is a network security system that acts as a barrier between a trusted internal network and untrusted external networks such as internet. It monitors and filters incoming and outgoing network traffic based on predefined security rules, effectively controlling what traffic is allowed to pass through.

**Network Vulnerabilities:** are weaknesses or flaws in a network hardware, software or organizational processes that can be exploited by cyber attackers to gain unauthorized access, disrupt operations, or steal data. These vulnerabilities can arise from various sources including:

* Misconfigured hardware
* Outdated software
* Weak security protocols
* Human error