UNIVERSITY OF KARACHI
DEPARTMENT OF COMPUTER SCIENCE
UBIT

RESEARCH FILE

RESEARCH TITLE:
NETWORK SECURITY ISSUES AND EFFECTIVE PROTECTION AGAINST NETWORK ATTACKS

SUBMITTED BY:
MEHAK FATIMA (B21110006057)
RIMSHA LARAIB (B21110006107)

SUBMITTED TO:
SIR BARI AHMED

Network Security Issues and Effective Protection Against Network Attacks

Rimsha Laraib, Mehak Fatima
Department Of Computer Science (UBIT)
University of Karachi

Abstract:

Networks are unsecured devices because of their basic feature of providing remote access and data communication. To provide effective communication and data sharing, we need to keep the network safe and secure. Due to the consequent threats and challenges faced in networks, network security has become one of the most important considerations in information technology infrastructures. Hackers and cybercriminals use malicious methods and tools to initiate network attacks and gain access to target organizations' assets. Network administrators and security experts use a variety of security technologies and techniques to guarantee network security.

Keywords: Network, network security, network attacks, network protection.

Introduction:

Network security has become a major problem in today's digitally connected world because of the increasing sophistication and frequency of attacks. These threats not only target the CIA's confidentiality, integrity, and availability of information but also pose serious risks to financial stability and organizational reputation. As attackers continue to exploit vulnerabilities in IT infrastructure, it is a must to implement robust security measures that restrict access to unauthorized users and protect sensitive data from misuse.

Unfortunately, detecting and mitigating cyber risks is not always straightforward, and failing to do so can result in serious consequences. According to a 2017 report, more than 2.6 billion data records were breached globally, with only 3.1% protected through encryption.

The core objective of network security is to prevent unauthorized access and protect digital assets from being exposed, altered, or destroyed. This is achieved through a combination of policies, tools, and technical safeguards designed by administrators to monitor, prevent, and respond to threats. Intrusion detection systems, firewalls, encryption, and access restrictions are some examples of these methods.

Failure to implement best security practices can lead to irrecoverable damage. Therefore, organizations need to stay up to date with the latest security measures to protect against potential attacks.

Literature Review:

Information Security Goals:

1. Confidentiality:

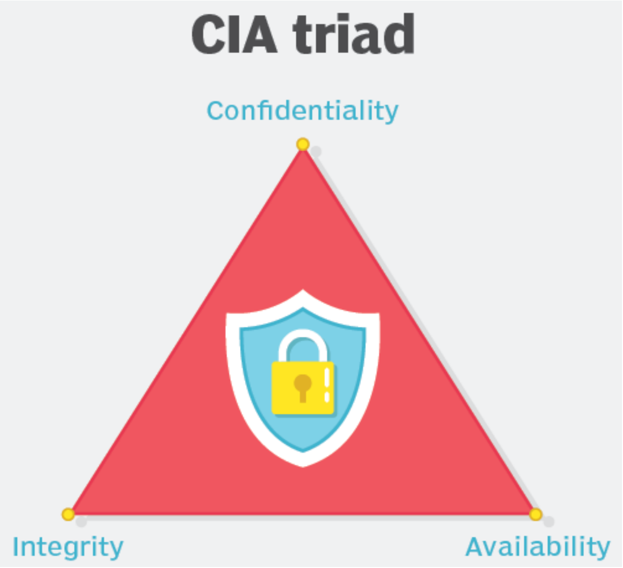
It ensures that data is accessible only to the authorized users and prevent it from unauthorized access.

2. Integrity:

Data must not be changed in transit, and steps must be taken to ensure it can't be altered by unauthorized people.

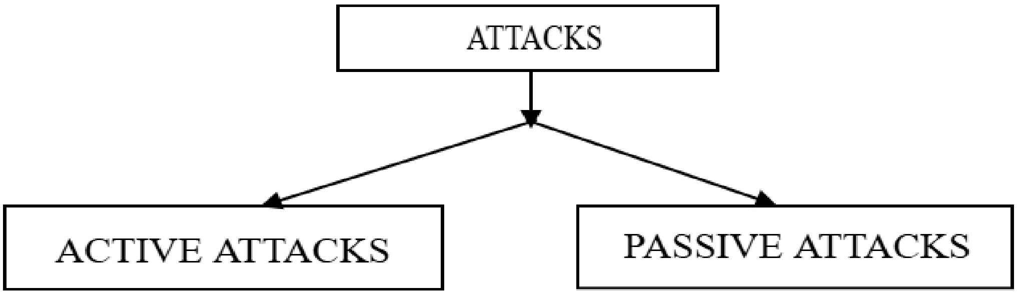
3. Availability:

Information should be accessible for authorized parties.



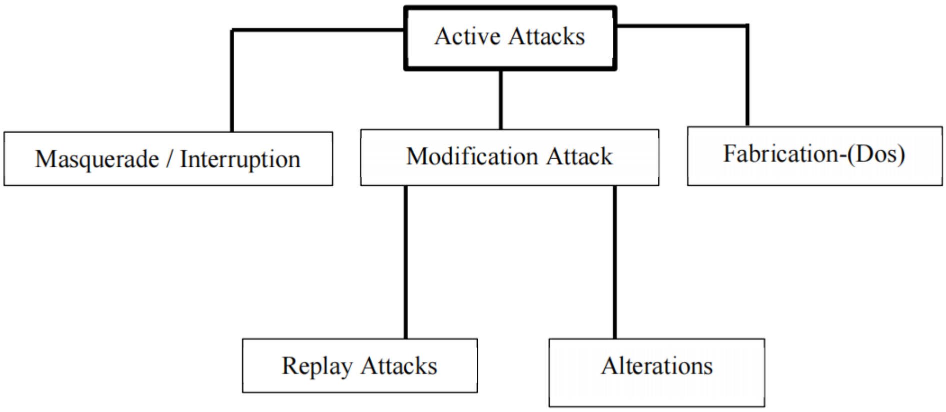
Attacks:

In network security an attack is any calculated action taken to compromise the confidentiality, integrity or availability of information or systems within a computer network.



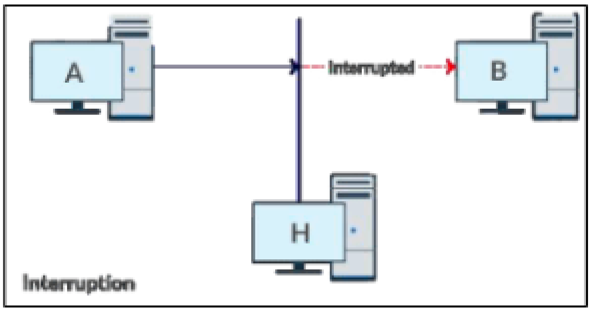
Active Attack:

An active attack is an attack in which attackers can read or modify the data. It can be easily identified due to the changes made by the attacker.



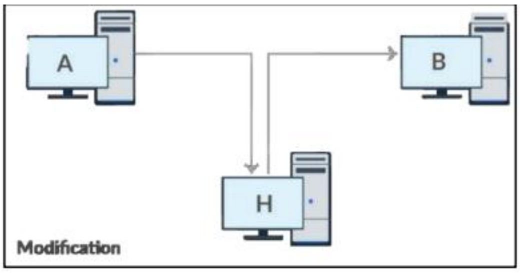
1. Masquerade/Interruption:

It is a type of active attack in which the attackers pretend to be someone to access systems or data.



2. Modification Attack:

It is an attack in which attacker alters the part of a message without permission.



2.1. Replay attacks:

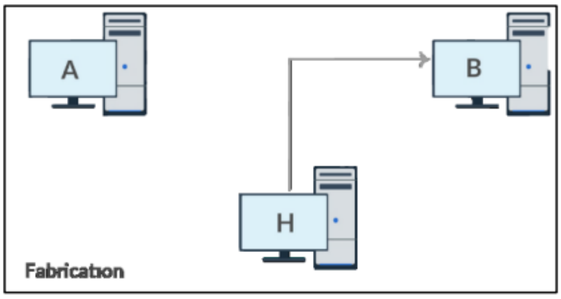
A replay attack is a network attack where an intercepted, valid data transmission is fraudulently repeated to deceive a system into performing unauthorized actions.

2.2. Alterations:

An alteration attack is a type of active network attack where the attacker modifies the content of data packet during transmission, in order to change its meaning or insert malicious content.

3. Fabrication:

A fabrication attack is when the attacker creates fake messages or data and sends them into a network to mislead the systems or users.

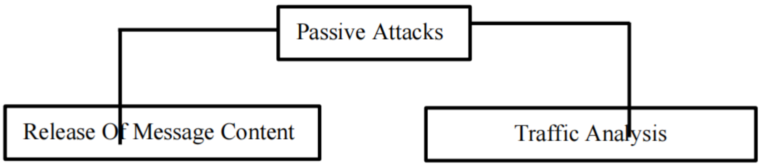


4. Denial of Service (Dos):

Denial of Service (DoS) is a type of active attack that prevents the system or network's intended users from accessing it by flooding traffic or requests.

Passive Attack:

It is an attack in which the attacker can only read the data secretly. It is hard to detect as it is a silent attack.



1. Release of Message Content:

It happens when a hacker reads private messages being sent over a network without permission.

2. Traffic Analysis:

It happens when a hacker does-not read the data but analyze the traffic to understand pattern like who is talking to whom.

Methodology:

This research adopts a qualitative methodology, examining available literature, case studies, and reported incidents to determine prevailing network security concerns and efficient protection approaches. The research aims at combining data from credible sources to give a broad overview of the topic.

Result:

Common Network Security Issues

1. **DoS attacks:** Denial of Service (DoS) is a type of active attack that prevents the system or network's intended users from accessing it by flooding traffic or requests.
2. **Password attacks:** An attempt to gain unauthorized access by cracking or stealing user passwords.
3. **URL interpretation:** A web-based attack that manipulates URLs to access restricted data or redirect users maliciously.
4. **Malware Attacks**: Malicious software designed to disrupt, damage, or gain unauthorized access to systems.
5. **Phishing Scams**: A cyberattack where attackers impersonate trusted entities to trick users into revealing sensitive information like passwords or credit card numbers.

Effective Protection Mechanisms

1. **Firewalls**: Act as barriers between trusted and untrusted networks, controlling incoming and outgoing traffic based on security rules.
2. **Intrusion Detection and Prevention Systems (IDPS)**: Monitor network traffic for suspicious activities and take action to prevent breaches.
3. **Encryption**: Secures data by converting it into unreadable code, accessible only with the correct decryption key.
4. **Regular Software Updates**: The routine process of installing the latest patches and improvements to fix security vulnerabilities and enhance system performance.

Discussion:

The finding from this paper highlights the increasing complexity of network security threats in modern digital environments. A single solution is not enough to address all security concerns effectively; rather, a hybrid approach could be essential. One of the most discussed methodologies is encryption, which ensures that sensitive data remains confidential and unreadable during transmission. It secures data but does not prevent unauthorized access or interruption. One key insight is that many of these attacks can be prevented or mitigated through the implementation of basic security practices, such as regular software updates, strong password policies, employee training, and the use of firewalls and intrusion detection systems.

Conclusion:

In conclusion, while technical solutions form the backbone of network defense, the human element must not be overlooked. A combination of strong security infrastructure, updated software, well-informed users, and proactive policies is essential for creating a resilient network environment in the face of ever-evolving threats.
The overall strategy in this case consists of the following three steps:
1- **Protection:** We need to configure our systems and network properly.
2- **Detection:** We must fully monitor the network and detect changes and the use of network resources that are signs of intrusion.
3- **Reaction:** Once identified problems, we need to respond to them quickly and quickly provide a secure environment on network.

References:

1. https://arxiv.org/pdf/1511.00568
2. https://hal.science/hal-03128076/
3. https://ieeexplore.ieee.org/document/9401544/authors#authors
4. https://www.academia.edu/77330568/A_Survey_on_Computer_and_Network_Security_Attacks
5. https://www.academia.edu/37580032/Network_Security_Survey_on_Network_Security_Threats_and_Attacks?auto=download
6. https://www.academia.edu/download/100604849/Network_Security_Concepts_Dangers_and_Defend_Best_Practical_PB.pdf
7. https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/
8. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA