Notes provided by Prakash Sir

Types of Attacks

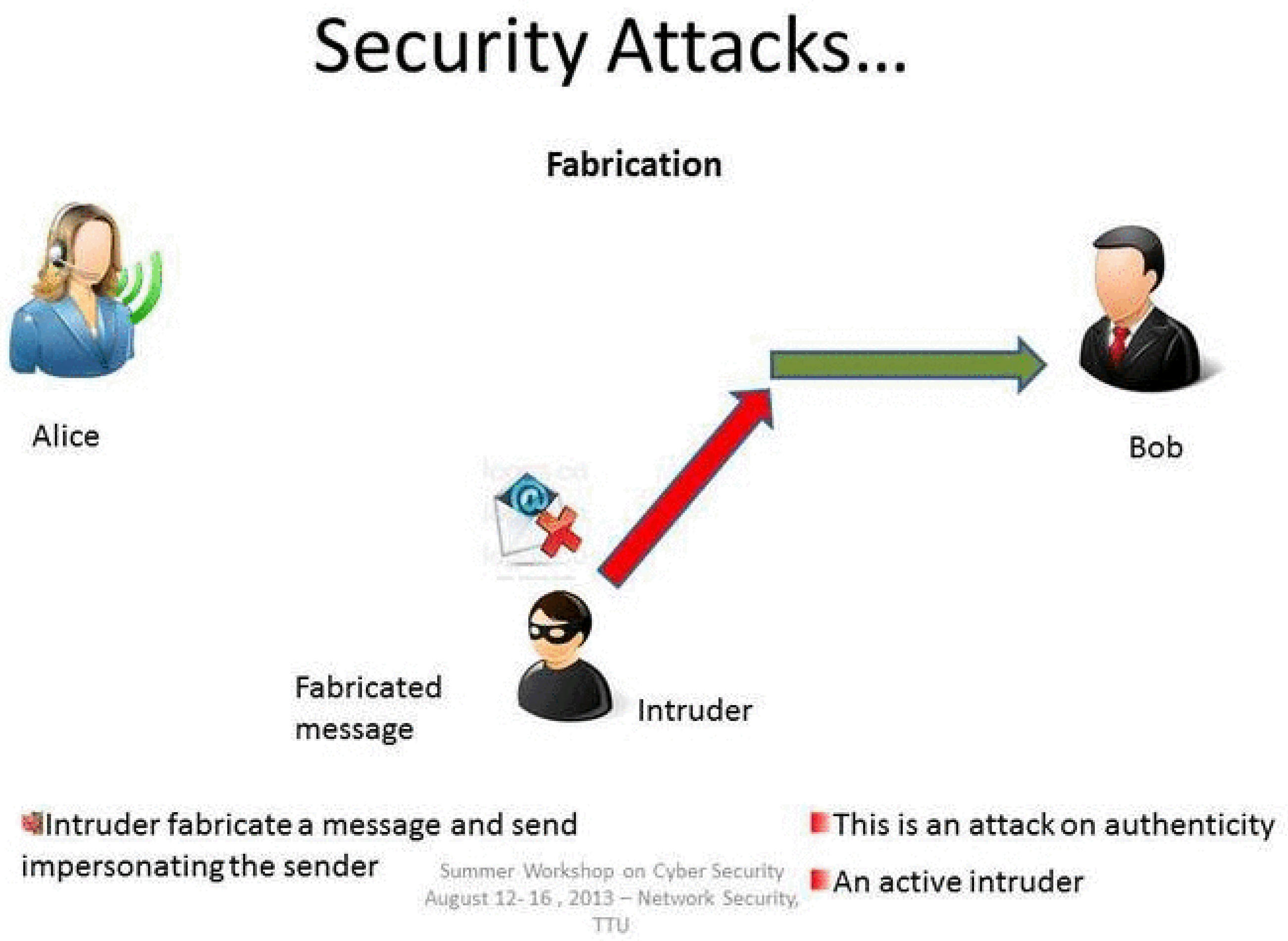
In an Information Security context there are 4 broad based categories of attacks:

1. Fabrication
2. Interception
3. Interruption
4. Modification

Fabrication

As stated above, *fabrication* is one of the four broad-based categories used to classify attacks and threats. A fabrication attack creates illegitimate information, processes, communications or other data within a system.

Often, fabricated data is inserted right alongside authentic data. When a known system is compromised, attackers may use fabrication techniques to gain trust, create a false trail, collect data for illicit use, spawn malicious or extraneous processes. In addition, fabricated data may reduce confidence in genuine data with the affected system.



Security Attacks...

Fabrication

- Intruder fabricate a message and send impersonating the sender
- This is an attack on authenticity
- An active intruder

Summer Workshop on Cyber Security August 12-16 , 2013 – Network Security, TTU

Figure 1
: Fabrication Attack. ("Secuity Attacks: Fabriaction" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0)

Examples of Fabrication attacks include:

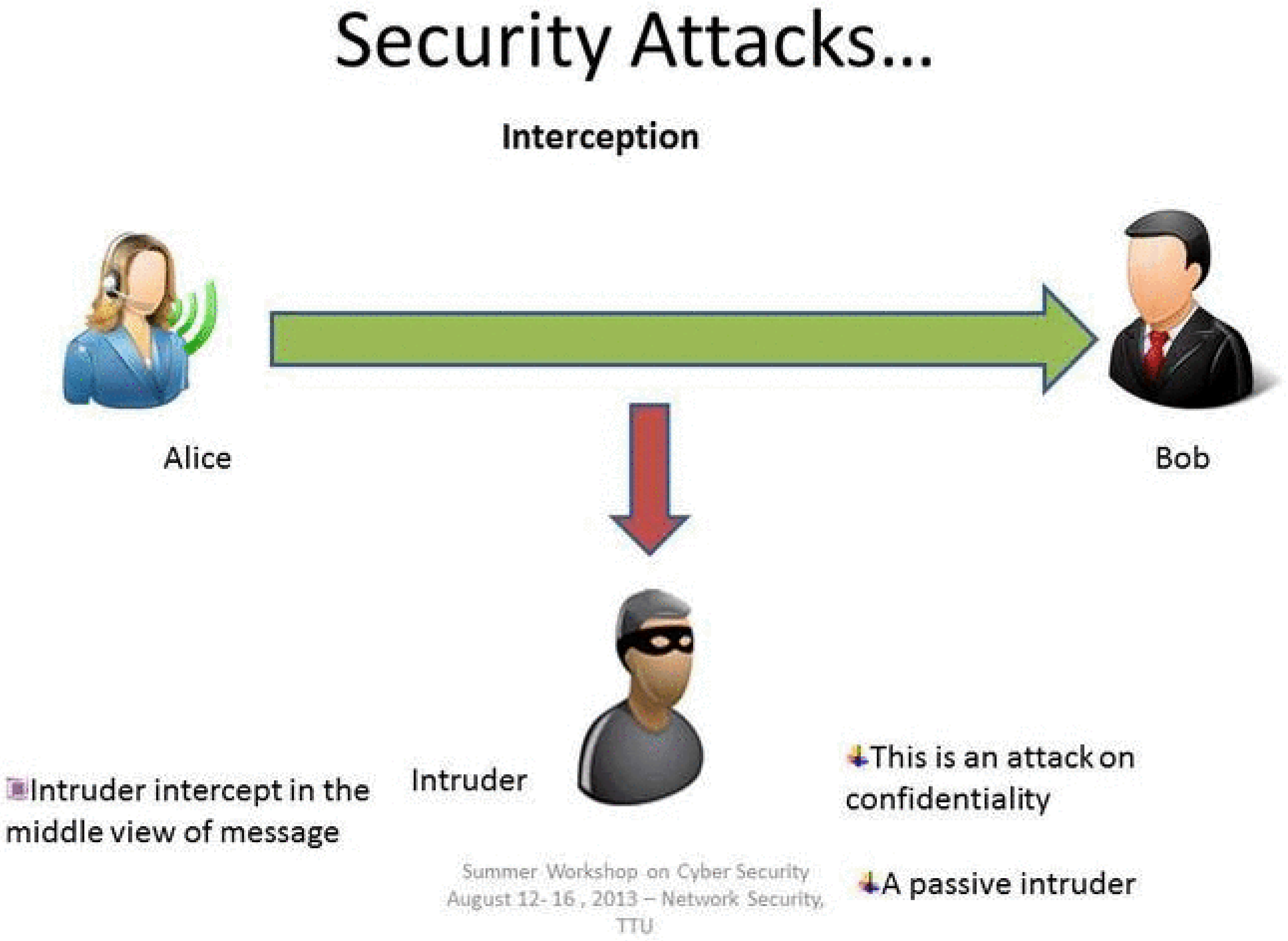
- SQL Injection
- Route Injection
- User / Credential Counterfeiting
- Log / Audit Trail Falsification
- Email Spoofing

Mitigate the attack :

- Use of Authentication and authorization mechanisms
- Using Firewalls
- Use Digital Signatures - Digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document.

Interception

An interception is where an unauthorized individual gains access to confidential or private information. **Interception attacks** are attacks against network the **confidentiality** objective of the CIA Triad.


Security Attacks…

Interception

Intruder intercept in the middle view of message

This is an attack on confidentiality

A passive intruder

Summer Workshop on Cyber Security August 12- 16 , 2013 – Network Security, TTU

Figure 1
: Interception Attacks. ("Security Attacks: Interception" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0)

Examples of Interception attacks:

- Eavesdropping on communication.
- Wiretapping telecommunications networks.
- Illicit copying of files or programs.
- Obtaining copies of messages for later replay.
- Packet sniffing and key logging to capture data from a computer system or network.

Mitigate the attack :

- Using Encryption - SSL, VPN, 3DES, BPI+ are deployed to encrypts the flow of information from source to destination so that if someone is able to snoop in on the flow of traffic, all the person will see is ciphered text.
- Traffic Padding - It is a function that produces cipher text output continuously, even in the absence of plain text. A continuous random data stream is generated. When plaintext is available, it is encrypted and transmitted. When input plaintext is not present, the random data are encrypted and transmitted. This makes it impossible for an attacker to distinguish between tree data flow and noise and therefore impossible to deduce the amount of traffic.

Interruption

In an interruption attack, a network service is made degraded or unavailable for legitimate use. They are the attacks against the availability of the network.

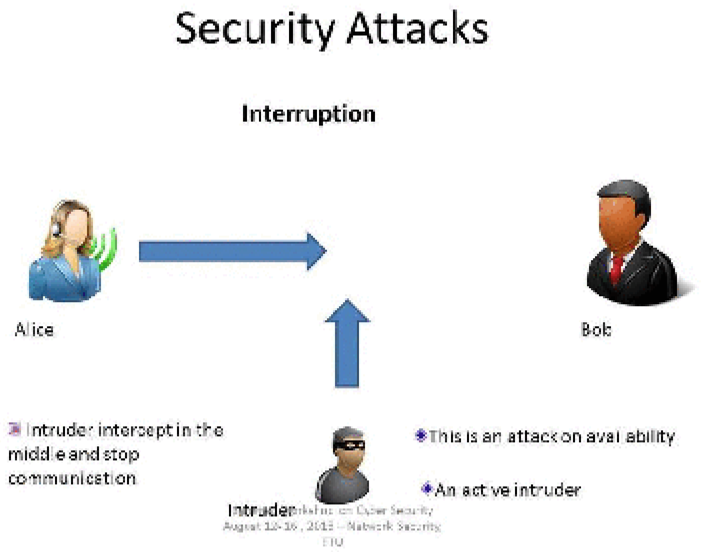

Security Attacks
Interruption
Alice
Bob
Intruder intercept in the middle and stop communication
This is an attack on availability
An active intruder
Intruder
Workshop on Cyber Security
August 12-16, 2013 – Network Security
FIU

Figure 1
: Interruption Attack. ("Security Attacks: Interruption" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0)

Examples of Interruption attacks :

- Overloading a server host so that it cannot respond.
- Cutting a communication line.
- Blocking access to a service by overloading an intermediate network or network device.
- Redirecting requests to invalid destinations.
- Theft or destruction of software or hardware involved.

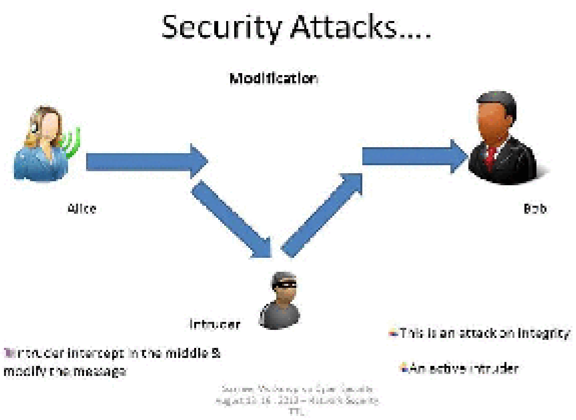
Mitigate the attack:

- Use Firewalls - Firewalls have simple rules such as to allow or deny protocols, ports or IP addresses. Modern stateful firewalls like Check Point FW1 NGX and Cisco PIX have a built-in capability to differentiate good traffic from DoS attack traffic.
- Keeping backups of system configuration data properly.
- Replication.

Modification

Modification is an attack against the integrity of the information. Basically there is three types of modifications.

- Change: Change existing information. The information is already existed but incorrect. Change attacks can be targeted at sensitive information or public information.
- Insertion: When an insertion attack is made, information that did not previously exist is added. This attack may be mounted against historical information or information that is yet to be acted upon.
- Deletion : Removal of existing information.


Security Attacks....

Modification

Alice
Bob
Intruder
Intruder intercept in the middle & modify the message
This is an attack on Integrity
An active intruder

Figure 1
: Modification Attack. ("Security Attacks: Modification" by Unknown, CS Dept - Texas Tech University is licensed under CC BY-SA 4.0)

Examples of Modification attacks include:

- Modifying the contents of messages in the network.
- Changing information stored in data files.
- Altering programs so they perform differently.
- Reconfiguring system hardware or network topologies.

Mitigate the attack :

- Introduction of intrusion detection systems (IDS) which could look for different signatures which represent an attack.
- Using Encryption mechanisms
- Traffic padding

- Keeping backups
- Use messaging techniques such as checksums, sequence numbers, digests, authentication codes

---

1. Back to top
    2.
    - 1.3 Models of Security - CIA / Parkerian Hexad
    - 1.5: Vulnerabilities

- Was this article helpful?

Title: Types of Attacks

Fabrication:

Fabrication attacks involve the creation of false or illegitimate information, processes, communications, or data within a system. These attacks are used to deceive, manipulate, or disrupt the target system. Some examples of fabrication attacks include SQL injection, route injection, user/credential counterfeiting, log/audit trail falsification, and email spoofing. To mitigate fabrication attacks, the following measures can be employed:

- Use of authentication and authorization mechanisms.

- Implement firewalls to filter and control network traffic.

- Utilize digital signatures to authenticate the origin and integrity of digital messages or documents.

Interception:

Interception attacks occur when unauthorized individuals gain access to confidential or private information, compromising the confidentiality aspect of the CIA Triad. Examples of interception attacks include eavesdropping on communications, wiretapping telecommunications networks, illicit copying of files or programs, obtaining copies of messages for later replay, and capturing data through packet sniffing and keylogging. To mitigate interception attacks, the following strategies can be applied:

- Employ encryption methods like SSL, VPN, 3DES, and BPI+ to protect data in transit.

- Utilize traffic padding techniques to obscure the volume of traffic and prevent attackers from distinguishing between data flow and noise.

Interruption:

Interruption attacks focus on degrading or disrupting network services, rendering them unavailable for legitimate use. These attacks target the availability of the network. Examples of interruption attacks include overloading a server host, cutting communication lines, blocking access by overloading network devices, redirecting requests to invalid destinations, and theft or destruction of software or hardware. Mitigation strategies for interruption attacks include:

- Using firewalls with the capability to differentiate legitimate traffic from denial of service (DoS) attack traffic.

- Keeping proper backups of system configuration data.

- Implementing replication for redundancy.

Modification:

Modification attacks aim to compromise the integrity of information by altering, inserting, or deleting data. There are three types of modifications: change, insertion, and deletion. Examples of modification attacks include changing the contents of messages in the network, altering information stored in data files, reconfiguring system hardware or network topologies, and modifying program behavior. To mitigate modification attacks, the following techniques can be employed:

- Introduction of intrusion detection systems (IDS) to detect attack signatures.

- Implement encryption mechanisms to protect data integrity.

- Utilize traffic padding to obfuscate data traffic.

- Maintain backups of data.

- Implement messaging techniques such as checksums, sequence numbers, digests, and authentication codes to verify data integrity.

These four broad categories of attacks encompass various threats and vulnerabilities in information security, and the mentioned mitigation strategies help protect against them.

Types of Attacks Cheatsheet

Fabrication

- Description: Fabrication attacks involve creating false or illegitimate information, processes, communications, or data within a system to deceive or disrupt.

- Examples: SQL injection, route injection, user/credential counterfeiting, log/audit trail falsification, email spoofing.

- Mitigation:

  - Use authentication and authorization mechanisms.

  - Implement firewalls to control network traffic.

  - Utilize digital signatures for message integrity.

Interception

- Description: Interception attacks compromise confidentiality by gaining unauthorized access to private information.

- Examples: Eavesdropping, wiretapping, illicit copying, packet sniffing, keylogging.

- Mitigation:

  - Use encryption methods (SSL, VPN, 3DES) to protect data in transit.

  - Employ traffic padding to obscure traffic volume.

Interruption

- Description: Interruption attacks disrupt network services, rendering them unavailable for legitimate use, focusing on availability.

- Examples: Overloading servers, cutting communication lines, blocking access, redirecting requests, theft or destruction.

- Mitigation:

  - Use firewalls to differentiate legitimate traffic from DoS attacks.

  - Maintain proper backups of system configuration data.

  - Implement replication for redundancy.

Modification

- Description: Modification attacks compromise data integrity by changing, inserting, or deleting information.

- Examples: Modifying messages, altering data files, reconfiguring hardware, changing program behavior.

- Mitigation:

  - Use intrusion detection systems (IDS) to detect attack signatures.

  - Implement encryption mechanisms to protect data integrity.

  - Utilize traffic padding to obfuscate data traffic.

  - Maintain backups of data.

  - Implement message verification techniques (checksums, sequence numbers, digests, authentication codes).

These attack categories encompass various threats in information security, and the mentioned mitigation strategies are crucial for protection.