


Motives, Goals, and Objectives of Information Security Attacks



Attacks = Motive (Goal) + Method + Vulnerability

- A motive originates out of the notion that the **target system stores or processes** something valuable, and this leads to the threat of an attack on the system
- Attackers try various tools and attack techniques to **exploit vulnerabilities** in a computer system or its security policy and controls in order to fulfil their motives

Motives behind information security attacks

<ul style="list-style-type: none">■ Disrupting business continuity■ Stealing information and manipulating data■ Creating fear and chaos by disrupting critical infrastructures■ Causing financial loss to the target	<ul style="list-style-type: none">■ Propagating religious or political beliefs■ Achieving a state's military objectives■ Damaging the reputation of the target■ Taking revenge■ Demanding ransom
---	--

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.


Motives, Goals, and Objectives of Information Security Attacks

Attackers generally have motives (goals), and objectives behind their information security attacks. A motive originates out of the notion that a target system stores or processes something valuable, which leads to the threat of an attack on the system. The purpose of the attack may be to disrupt the target organization's business operations, to steal valuable information for the sake of curiosity, or even to exact revenge. Therefore, these motives or goals depend on the attacker's state of mind, their reason for carrying out such an activity, as well as their resources and capabilities. Once the attacker determines their goal, they can employ various tools, attack techniques, and methods to exploit vulnerabilities in a computer system or security policy and controls.

Attacks = Motive (Goal) + Method + Vulnerability

Motives behind information security attacks

- | | |
|---|---|
| <ul style="list-style-type: none">■ Disrupt business continuity■ Perform information theft■ Manipulating data■ Create fear and chaos by disrupting critical infrastructures■ Bring financial loss to the target | <ul style="list-style-type: none">■ Propagate religious or political beliefs■ Achieve a state's military objectives■ Damage the reputation of the target■ Take revenge■ Demand ransom |
|---|---|

Classification of Attacks		
Passive Attacks	<ul style="list-style-type: none">Passive attacks do not tamper with the data and involve intercepting and monitoring network traffic and data flow on the target networkExamples include sniffing and eavesdropping	
Active Attacks	<ul style="list-style-type: none">Active attacks tamper with the data in transit or disrupt the communication or services between the systems to bypass or break into secured systemsExamples include DoS, Man-in-the-Middle, session hijacking, and SQL injection	
Close-in Attacks	<ul style="list-style-type: none">Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or disrupt access to informationExamples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving	
Insider Attacks	<ul style="list-style-type: none">Insider attacks involve using privileged access to violate rules or intentionally cause a threat to the organization's information or information systemsExamples include theft of physical devices and planting keyloggers, backdoors, and malware	
Distribution Attacks	<ul style="list-style-type: none">Distribution attacks occur when attackers tamper with hardware or software prior to installationAttackers tamper with the hardware or software at its source or in transit	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Classification of Attacks

According to IATF, security attacks are classified into five categories: passive, active, close-in, insider, and distribution.

▪ Passive Attacks

Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data. Attackers perform reconnaissance on network activities using sniffers. These attacks are very difficult to detect as the attacker has no active interaction with the target system or network. Passive attacks allow attackers to capture the data or files being transmitted in the network without the consent of the user. For example, an attacker can obtain information such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks.

Examples of passive attacks:

- Footprinting
- Sniffing and eavesdropping
- Network traffic analysis
- Decryption of weakly encrypted traffic

▪ Active Attacks

Active attacks tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems. Attackers launch attacks on the target system or network by sending traffic actively that can be detected. These

attacks are performed on the target network to exploit the information in transit. They penetrate or infect the target's internal network and gain access to a remote system to compromise the internal network.

Examples of active attacks:

- Denial-of-service (DoS) attack
- Bypassing protection mechanisms
- Malware attacks (such as viruses, worms, ransomware)
- Modification of information
- Spoofing attacks
- Replay attacks
- Password-based attacks
- Session hijacking
- Man-in-the-Middle attack
- DNS and ARP poisoning
- Compromised-key attack
- Firewall and IDS attack
- Profiling
- Arbitrary code execution
- Privilege escalation
- Backdoor access
- Cryptography attacks
- SQL injection
- XSS attacks
- Directory traversal attacks
- Exploitation of application and OS software

▪ **Close-in Attacks**

Close-in attacks are performed when the attacker is in close physical proximity with the target system or network. The main goal of performing this type of attack is to gather or modify information or disrupt its access. For example, an attacker might shoulder surf user credentials. Attackers gain close proximity through surreptitious entry, open access, or both.

Examples of close-in attacks:

- Social engineering (Eavesdropping, shoulder surfing, dumpster diving, and other methods)

▪ **Insider Attacks**

Insider attacks are performed by trusted persons who have physical access to the critical assets of the target. An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems. Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information. They misuse the organization's assets to directly affect the confidentiality, integrity, and availability of information systems. These attacks impact the organization's business operations, reputation, and profit. It is difficult to figure out an insider attack

Examples of insider attacks:

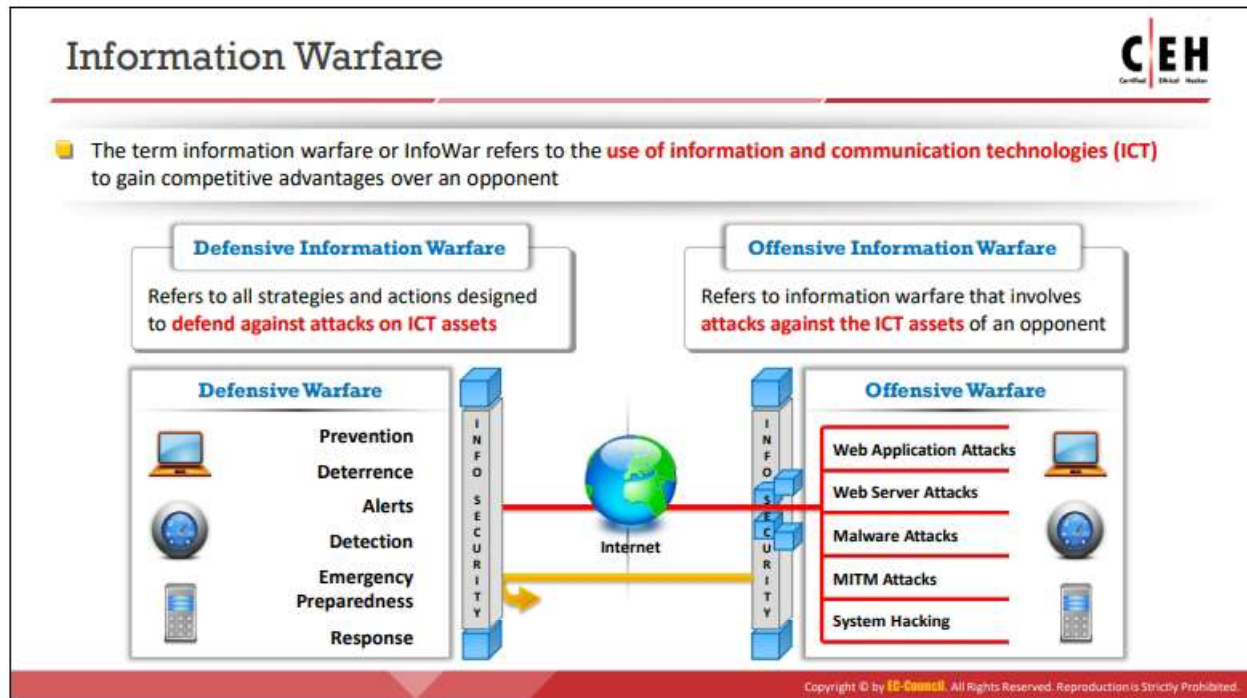
- Eavesdropping and wiretapping

- Theft of physical devices
- Social engineering
- Data theft and spoliation
- Pod slurping
- Planting keyloggers, backdoors, or malware

▪ **Distribution Attacks**

Distribution attacks occur when attackers tamper with hardware or software prior to installation. Attackers tamper the hardware or software at its source or when it is in transit. Examples of distribution attacks include backdoors created by software or hardware vendors at the time of manufacture. Attackers leverage these backdoors to gain unauthorized access to the target information, systems, or network.

- Modification of software or hardware during production
- Modification of software or hardware during distribution



Information Warfare

Source: <http://www.iwar.org.uk>

The term information warfare or InfoWar refers to the use of information and communication technologies (ICT) for competitive advantages over an opponent. Examples of information warfare weapons include viruses, worms, Trojan horses, logic bombs, trap doors, nanomachines and microbes, electronic jamming, and penetration exploits and tools.

Martin Libicki divided information warfare into the following categories:

- **Command and control warfare (C2 warfare):** In the computer security industry, C2 warfare refers to the impact an attacker possesses over a compromised system or network that they control.
- **Intelligence-based warfare:** Intelligence-based warfare is a sensor-based technology that directly corrupts technological systems. According to Libicki, “intelligence-based warfare” is warfare that consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battlespace.
- **Electronic warfare:** According to Libicki, electronic warfare uses radio-electronic and cryptographic techniques to degrade communication. Radio electronic techniques attack the physical means of sending information, whereas cryptographic techniques use bits and bytes to disrupt the means of sending information.
- **Psychological warfare:** Psychological warfare is the use of various techniques such as propaganda and terror to demoralize one’s adversary in an attempt to succeed in battle.
- **Hacker warfare:** According to Libicki, the purpose of this type of warfare can vary from the shutdown of systems, data errors, theft of information, theft of services, system

monitoring, false messaging, and access to data. Hackers generally use viruses, logic bombs, Trojan horses, and sniffers to perform these attacks.

- **Economic warfare:** Libicki notes that economic information warfare can affect the economy of a business or nation by blocking the flow of information. This could be especially devastating to organizations that do a lot of business in the digital world.
- **Cyberwarfare:** Libicki defines cyber warfare as the use of information systems against the virtual personas of individuals or groups. It is the broadest of all information warfare. It includes information terrorism, semantic attacks (similar to Hacker warfare, but instead of harming a system, it takes over the system while maintaining the perception that it is operating correctly), and simula-warfare (simulated war, for example, acquiring weapons for mere demonstration rather than actual use).

Each form of information warfare mentioned above consists of both defensive and offensive strategies.

- **Defensive Information Warfare:** Involves all strategies and actions to defend against attacks on ICT assets.
- **Offensive Information Warfare:** Involves attacks against the ICT assets of an opponent.

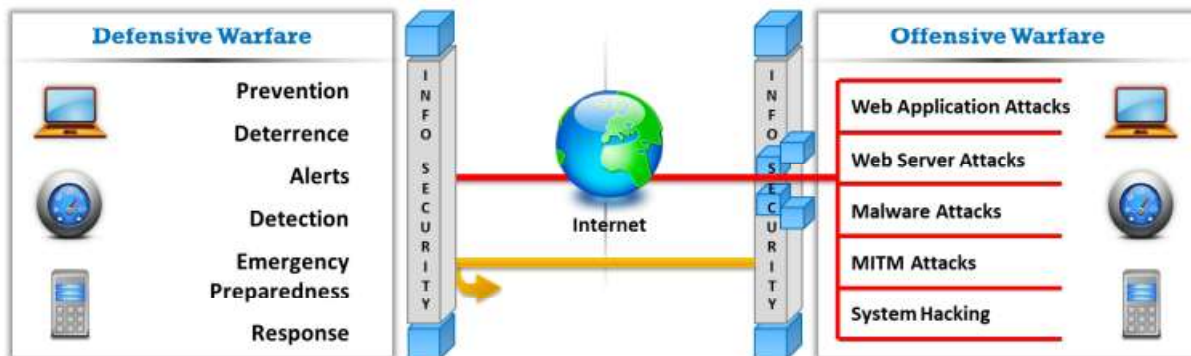


Figure 1.1: Block Diagram of Information Warfare