Cybersecurity: Concepts, Attacks, Techniques

Introduction to Cybersecurity

PORA
ACADEMY

Concepts: CIA Triad

Concepts: CIA Triad

The CIA triad is the cybersecurity principle that provides a high-level framework for cybersecurity professionals to consider when auditing, implementing, and improving systems, tools, and programs for organizations. It's comprised of the three Cybersecurity pillars:

- Confidentiality
- Integrity
- Availability

Concepts: CIA Triad

- By ensuring confidentiality, integrity, and availability, organizations can safeguard against unauthorized access, data corruption, and disruptions in service.

Concepts: CIA Triad - Confidentiality

- Confidentiality ensures that sensitive information is only accessible to those authorized to view it. Protecting data from unauthorized access is critical in industries that handle personal, financial, or classified information.

- In the healthcare industry, patient records must remain confidential to protect patients' privacy. In finance, customer account details must be kept confidential to prevent identity theft and fraud.

Concepts: CIA Triad - Confidentiality

- Maintaining confidentiality involves challenges such as preventing unauthorized access, managing insider threats, and protecting against data breaches. Encryption, access control policies, and regular audits are common strategies used to address these challenges.

Concepts: CIA Triad - Integrity

- Integrity ensures that data remains accurate, complete, and reliable throughout its lifecycle. It protects against unauthorized modifications that could lead to misinformation, financial loss, or legal consequences.

- In financial services, integrity is crucial for ensuring that transactions are accurately recorded and account balances are correct. In legal contexts, document integrity is essential for ensuring that contracts and agreements are enforceable.

Concepts: CIA Triad - Integrity

- Integrity can be compromised by cyberattacks such as data tampering or by human error. To protect data integrity, organizations use methods such as cryptographic hash functions, digital signatures, and rigorous validation processes.

Concepts: CIA Triad - Availability

- Availability ensures that information and resources are accessible to authorized users whenever needed. This principle is particularly important for services that must operate continuously, such as emergency response systems and online services.

- E-commerce platforms must ensure availability to handle transactions at any time, especially during high-demand periods like holiday sales. Similarly, availability is critical for online banking services, where users expect uninterrupted access to their accounts.

Concepts: CIA Triad - Availability

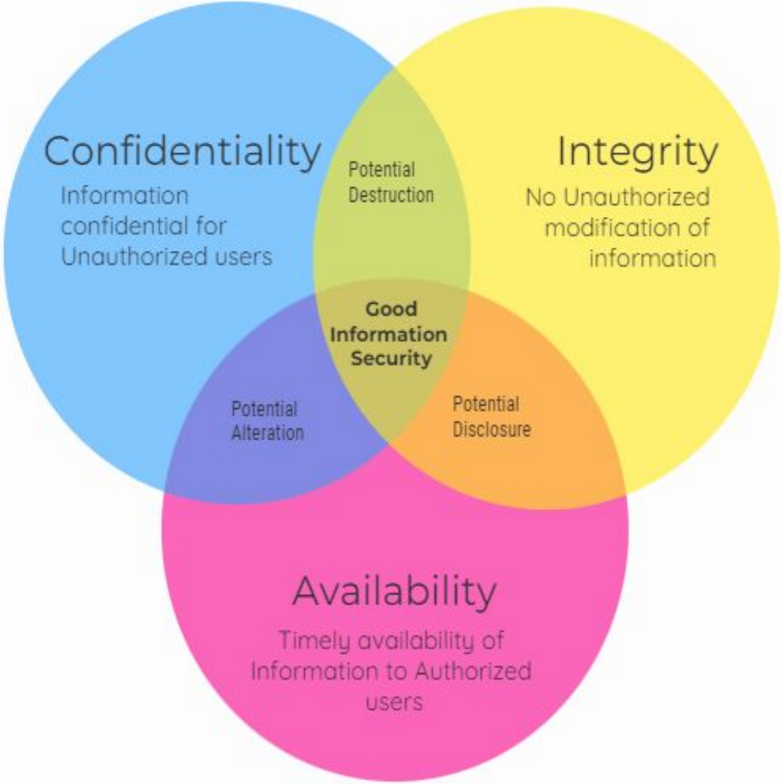
- Availability can be threatened by factors such as Distributed Denial of Service (DDoS) attacks, hardware failures, or natural disasters. Strategies to ensure availability include redundancy, failover systems, and regular maintenance.
-

Concepts: CIA Triad Interdependence

- Confidentiality, Integrity, and Availability are interrelated and must be balanced. For example, securing the confidentiality of data may involve encryption, which also needs to maintain the integrity and availability of that data.
- A system that emphasizes availability may have to reduce some aspects of confidentiality to ensure that data is always accessible when needed. Conversely, focusing too much on confidentiality might reduce the system's availability due to stringent access controls.

cepts: CIA vs DAD

- Disclosure: Unauthorized access or exposure of confidential information.
- Impact: Breach of Confidentiality
- Alteration: Unauthorized modification or corruption of data.
- Impact: Breach of Integrity
- Denial: Interruption or denial of access to information and resources.
- Impact: Breach of Availability


Confidentiality
Information confidential for Unauthorized users
Integrity
No Unauthorized modification of information
Availability
Timely availability of Information to Authorized users
Potential Destruction
Potential Alteration
Potential Disclosure
Good Information Security

Concepts: Case Study 1

The CIA Triad in Healthcare

Scenario: A large hospital network implements an Electronic Health Record (EHR) system to digitize patient records and improve care coordination. The implementation focuses on ensuring confidentiality, integrity, and availability.

Confidentiality: The hospital uses encryption to protect patient data, ensuring that only authorized healthcare providers can access the records. Access controls are implemented, allowing different levels of data access based on roles within the organization.

Integrity: To maintain the integrity of patient records, the EHR system includes audit trails that track changes made to records. Any modification must be validated and authorized, ensuring that the data remains accurate and reliable.

Availability: The hospital ensures that the EHR system is highly available by using redundant servers, disaster recovery plans, and regular system backups. This guarantees that patient records are accessible even during emergencies.

Outcome: The hospital successfully protected patient data while ensuring that healthcare providers had reliable access to accurate information, improving patient care and operational efficiency.

Concepts: Case Study 2

The CIA Triad in Financial Services

Scenario:A global bank launches a new online banking platform that must adhere to the principles of the CIA Triad to protect customer data and maintain trust.

Confidentiality:The bank implements end-to-end encryption for all online transactions and data transfers, ensuring that customer information is protected from unauthorized access. Multi-factor authentication (MFA) is required for all users to enhance security.

Integrity:Transaction records are protected using cryptographic hash functions, ensuring that any tampering would be immediately detected. Regular audits and reconciliation processes are also in place to maintain data integrity.

Availability:The bank invests in a robust infrastructure with load balancing and failover systems to ensure that online banking services are always available, even during peak times or cyberattacks.

Outcome:The platform successfully maintained customer trust by providing secure, reliable access to financial services, ensuring the protection of sensitive data while remaining highly available.

Concepts: Case Study 3

The CIA Triad in E-Commerce

Scenario:A leading e-commerce platform implements the CIA Triad principles to secure online transactions and maintain service reliability during high-traffic events like holiday sales.

Confidentiality:Customer information, including payment details, is encrypted both at rest and in transit. The platform also restricts access to sensitive data, ensuring that only authorized personnel can view or process it.

Integrity:The accuracy of product information, pricing, and order details is ensured through strict data validation processes. Any changes to data are logged and reviewed to prevent tampering.

Availability:The platform prepares for high traffic by using scalable cloud infrastructure, content delivery networks (CDNs), and DDoS protection to ensure that the site remains available to customers even during peak periods.

Outcome:The e-commerce platform maintained a seamless shopping experience, securing transactions and keeping the platform operational during critical sales events, resulting in high customer satisfaction and trust.

Cybersecurity Attacks: The Cyber Kill Chain

Cybersecurity Attacks

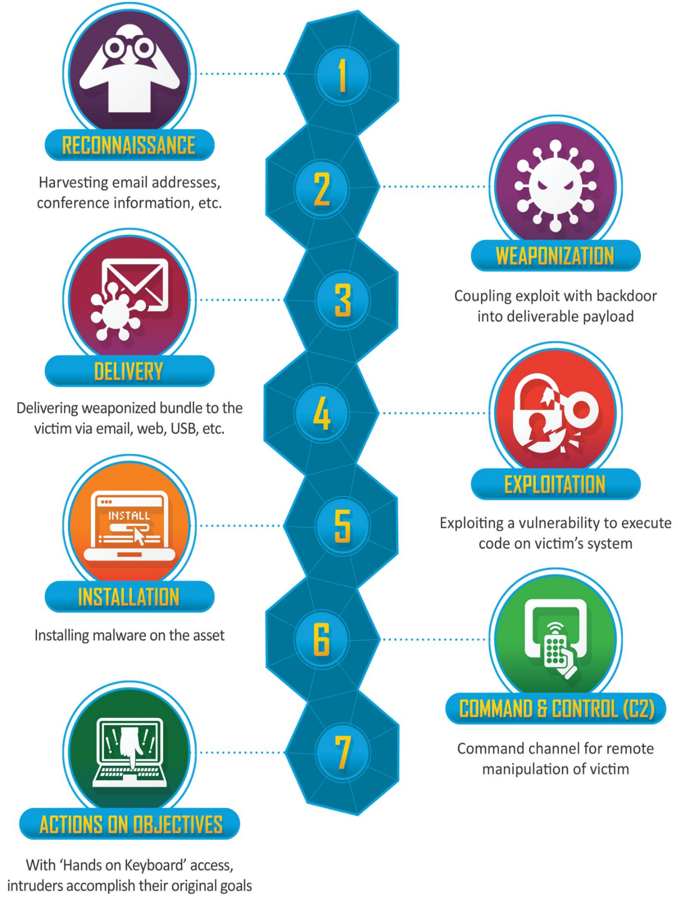
Introduction to Cybersecurity Attacks

- Cybersecurity attacks involve attempts to exploit systems and data.
- The Cyber Kill Chain helps categorize and defend against attacks.
- We will explore how common cyberattacks fit into each stage, including unethical techniques and attacks like DoS and DDoS.

Cybersecurity Attacks: The Cyber Kill Chain

What is the Cyber Kill Chain?

- A seven-stage model developed to break down cyberattacks.
- Each stage offers an opportunity for defenders to detect and stop the attack.
- Understanding common attacks for each stage is crucial to strengthening defense.



1 RECONNAISSANCE

Harvesting email addresses, conference information, etc.

2 WEAPONIZATION

Coupling exploit with backdoor into deliverable payload

3 DELIVERY

Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION

Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION

Installing malware on the asset

6 COMMAND & CONTROL (C2)

Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES

With 'Hands on Keyboard' access, intruders accomplish their original goals

Cybersecurity Attacks: The Cyber Kill Chain

Stages of the Cyber Kill Chain

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives

Cybersecurity Attacks: The Cyber Kill Chain

Stage 1: Reconnaissance

Definition: Attackers gather information on the target.

Common Attacks and Techniques:

- Phishing campaigns
- Google dorking
- Social engineering
- DNS brute-forcing

Example: APT10 (Cloud Hopper) – Gaining access to cloud providers via reconnaissance.

Cybersecurity Attacks: The Cyber Kill Chain

Stage 2: Weaponization

Definition: Attackers create a malware payload combined with an exploit.

Common Attacks and Techniques:

- Weaponized PDFs and Office documents
- Exploit kits (e.g., Angler Exploit Kit)
- Zero-day exploits

Example: Stuxnet – Weaponized a zero-day exploit to target Iran's nuclear facilities.

Cybersecurity Attacks: The Cyber Kill Chain

Stage 3: Delivery

Definition: Delivering the payload to the victim.

Common Attacks and Techniques:

- Spear phishing
- Drive-by downloads
- USB infections
- DoS and DDoS attacks

Example: Mirai Botnet – Used IoT devices to disrupt services with a DDoS attack.

Cybersecurity Attacks: The Cyber Kill Chain

Stage 4: Exploitation

- Definition: The malware exploits a vulnerability in the system to execute.
- Common Attacks and Techniques:
  - Buffer overflow attacks
  - SQL injection
  - Cross-site scripting (XSS)
  - Privilege escalation
- Example: WannaCry – Used the EternalBlue exploit to spread ransomware.

Cybersecurity Attacks: The Cyber Kill Chain

Stage 5: Installation

- Definition: Malware installs itself and maintains a foothold in the system.
- Common Attacks and Techniques:
  - Trojans (e.g., Emotet)
  - Remote Access Trojans (RATs)
  - Rootkits
  - Web shells
- Example: Ghost RAT – Gained persistent access to systems to steal data.

Cybersecurity Attacks: The Cyber Kill Chain

Stage 6: Command and Control (C2)

- Definition: Attackers remotely control infected systems to execute further attacks.
- Common Attacks and Techniques:
  - Botnets (e.g., Zeus)
  - C2 servers
  - Domain Generation Algorithms (DGA)
  - DNS Tunneling
- Example: Zeus Botnet – Stole banking information using a C2 infrastructure.

Cybersecurity Attacks: The Cyber Kill Chain

Stage 7: Actions on Objectives

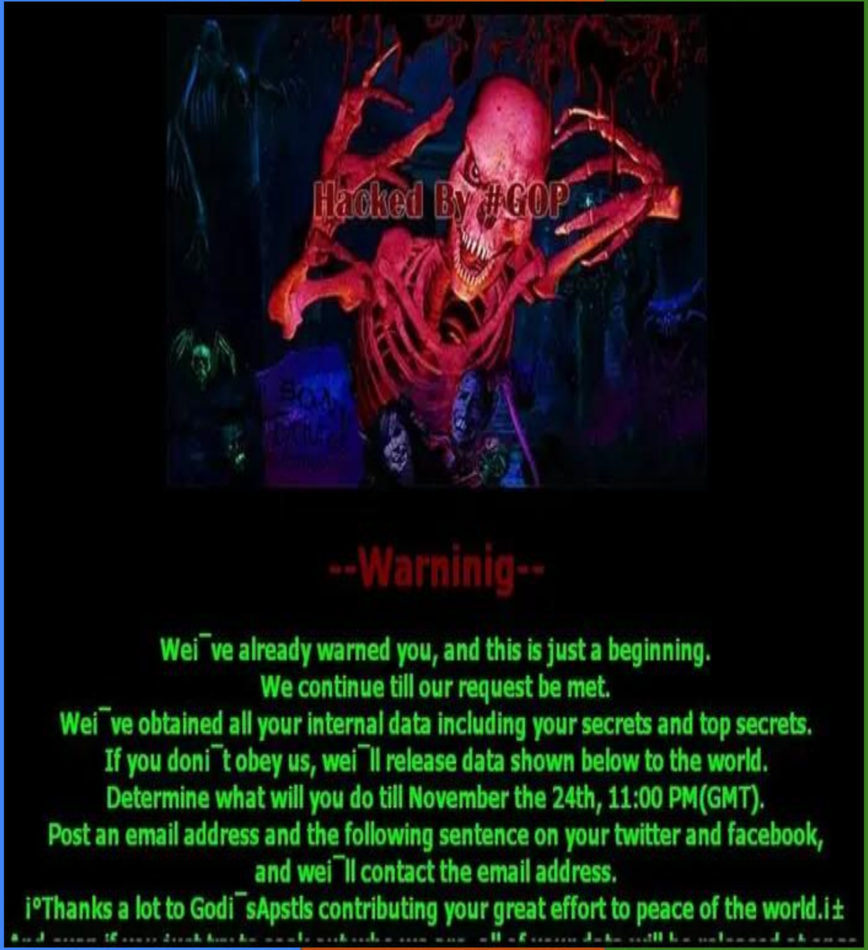
- Definition: Attackers complete their mission, whether data theft, destruction, or further attacks.
- Common Attacks and Techniques:
  - Data exfiltration (e.g., Equifax breach)
  - Ransomware (e.g., Maze ransomware)
  - Sabotage (e.g., NotPetya)
- Example: SolarWinds Hack – Exfiltrated data from high-profile targets for months.

Cybersecurity Attacks: The Cyber Kill Chain

Real-World Example of an Attack

- Example: Sony Hack – Attackers used spear-phishing, installed malware, and leaked sensitive data.
- Lessons Learned: Early detection, patch management, and effective incident response are critical.

Sony hack - more info



Hacked By #GOP

--Warninig--

Wei¯ve already warned you, and this is just a beginning.
We continue till our request be met.
Wei¯ve obtained all your internal data including your secrets and top secrets.
If you doni¯t obey us, wei¯ll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Post an email address and the following sentence on your twitter and facebook,
and wei¯ll contact the email address.
i°Thanks a lot to Godi¯sApstls contributing your great effort to peace of the world.i±

PORA ACADEMY

Cyber Security Techniques: The Cyber Kill Chain

Cyber Security Techniques: The Cyber Kill Chain

- Cybersecurity techniques are essential in preventing, detecting, and mitigating cyberattacks.
- In this presentation, we will explore security techniques mapped to each stage of the Cyber Kill Chain, along with examples and real-world use cases.

Cyber Security Techniques: The Cyber Kill Chain

Reconnaissance: Attackers gather information about the target.

Common Security Techniques:

- User Awareness Training

- Access Control

- Deception Technologies (Honeypots)

Example: Google conducts phishing simulations to help employees recognize phishing attacks.

Link: [Google and Phishing Simulation]

Cyber Security Techniques: The Cyber Kill Chain

Weaponization: Attackers create malicious payloads using exploits.

Common Security Techniques:

- Patch Management
- Secure Coding Practices
- Code Review and Testing

Example: Equifax data breach resulted from a missed security patch for Apache Struts.

Link: [Equifax Data Breach Analysis]

Cyber Security Techniques: The Cyber Kill Chain

Delivery: Attackers deliver the malicious payload via phishing, websites, or USB devices.

Common Security Techniques:

- Multi-Factor Authentication (MFA)

- Network Segmentation

- Email Filtering

Example: Dropbox uses MFA to prevent unauthorized access even if a password is compromised.

Link: [Dropbox MFA Security Overview]

Cyber Security Techniques: The Cyber Kill Chain

Exploitation: Attackers exploit vulnerabilities to gain unauthorized access.

Common Security Techniques:

- Least Privilege

- Vulnerability Scanning

- Application Hardening

Example: AWS uses the principle of least privilege to secure cloud resources.

Link: [AWS Least Privilege Security Approach]

Cyber Security Techniques: The Cyber Kill Chain

Installation: Attackers install backdoors or malware to maintain persistent access.

Common Security Techniques:

- Application Whitelisting

- Change Control Processes

- File Integrity Monitoring (FIM)

Example: McAfee Application Control helps companies implement application whitelisting.

Link: [McAfee Application Control for Whitelisting]

Cyber Security Techniques: The Cyber Kill Chain

Command and Control: Attackers establish communication with compromised systems.

Common Security Techniques:

- DNS Filtering
- Outbound Traffic Filtering
- Anomaly Detection

Example: Cisco Umbrella uses DNS filtering to block attempts at C2 communication.

Link: [Cisco Umbrella DNS Filtering]

Cyber Security Techniques: The Cyber Kill Chain

Actions on Objectives: Attackers steal, encrypt, or disrupt sensitive data or systems.

Common Security Techniques:

- Data Encryption

- Data Loss Prevention (DLP)

- Incident Response Plans

Example: Google encrypts all data in transit across its cloud platform to protect customer information.

Link: [Google Cloud Encryption]

Cyber Security Techniques: The Cyber Kill Chain

Cross-Stage Techniques

Some security techniques apply across multiple stages of the Cyber Kill Chain.

Common Security Techniques:

- Multi-Factor Authentication (MFA)

- Least Privilege

- Encryption

Example: MFA prevents unauthorized access in the Delivery, Exploitation, and other stages.

The END

PORA ACADEMY