Topic 1

Introduction To Cybersecurity

Slides developed by

What you will learn in these slides...

- Overview of cybersecurity
- Common terms used in cybersecurity
  - Asset, Vulnerability, Risk, Threat
- CIA Triad and AAA Model
- Access control measures

A Brief Explanation of Cybersecurity

YouTube Link: https://www.youtube.com/watch?v=1vV0t2XbtuU

Overview of Cybersecurity

- Protecting/Safeguarding digital assets from cyber threats
  - Digital assets include computer systems, networks, websites etc.
- Implementing measures to help with protecting these systems
- Educating individuals and organizations about the importance of cybersecurity practices
  - Prevent financial losses
  - Ensure everyone plays their part in keeping their businesses threat-free

Foundational Concepts in Cybersecurity

- Asset, Vulnerability, Risk, Threat
- CIA Triad
- AAA Model
- Types of access control measures

Asset

- Any valuable resource that needs to be protected
- Can be physical or digital
  - Physical assets: Computers, laptops, hardware items
  - Digital assets: Data, software applications
- It is a good practice to classify assets on importance
  - Organizations can allocate resources more effectively to protect more valuable assets

Vulnerability

- A weakness or flaw in a system that can be exploited by threats
  - Can arise from software bugs, misconfigurations, design flaws or human errors
- Preventing and mitigating vulnerabilities
  - Conduct vulnerability assessments
  - Patch and update software regularly
  - Conduct regular security testing on systems and devices

Risk

- The potential for harm, loss or damage caused from a vulnerability exploit
- Often measured by
  - Likelihood of a situation occurring
  - Magnitude of the potential consequences
- Benefits of managing risks
  - Organizations can prioritize the risks to be addressed first, based on the risk matrix (next slide)

Risk Matrix

LIKELIHOOD \ MAGNITUDE	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Medium	Medium	Medium High	High	High
Likely	Low	Low Medium	Medium	Medium High	High
Possible	Low	Low Medium	Medium	Medium High	Medium High
Unlikely	Low	Low Medium	Low Medium	Medium	Medium High
Very Unlikely	Low	Low	Low Medium	Medium	Medium

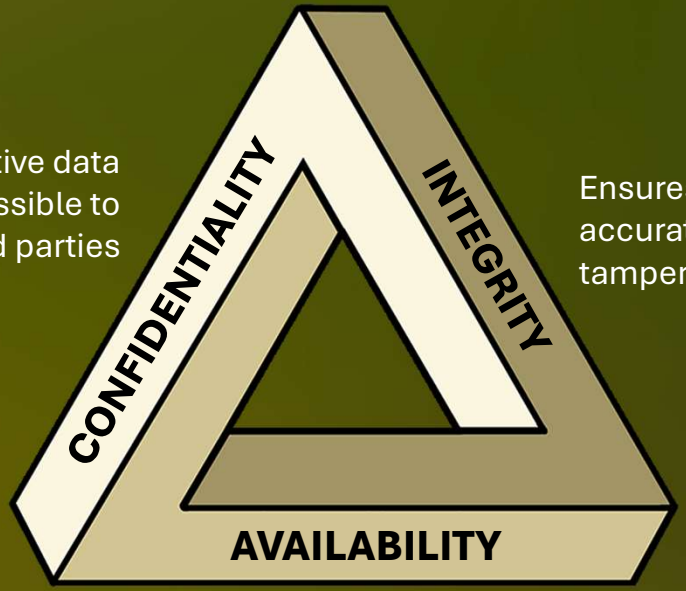
- Likelihood and Magnitude levels are often numbered 1 to 5
  - A level of 1 means Very Unlikely/Negligible while 5 means Very Likely/Severe
- **Risk Score** is calculated by multiplying Likelihood by Magnitude
  - A higher risk score indicates a riskier threat identified

Threat

- Any potential danger, hazard or malicious actor that seeks to exploit vulnerabilities and cause harm to assets
- Examples of threats include
  - Malware infections (will be covered in Topic 4)
  - Data breach
  - Insider threat
- How to defend against threats
  - Understand the nature and capabilities of threats
  - Stay informed about emerging threats and evolving attack techniques
  - Organizations should implement proactive security measures

CIA Triad

Ensure that sensitive data is only accessible to authorized parties



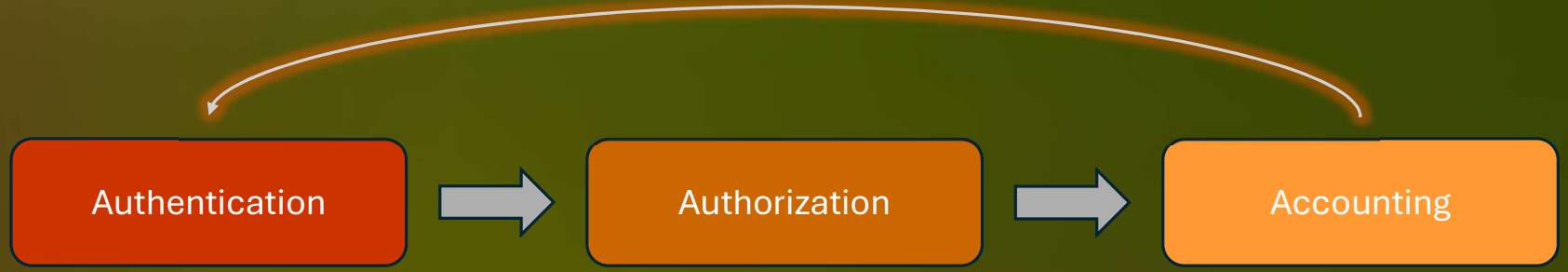
Ensures that data remains accurate and consistent (not tampered with)

Ensures that data will always be available to authorized users whenever needed

Importance of CIA Triad

- Offers a structured approach to addressing fundamental security objectives
- Allow organizations/individuals to identify and mitigate a wide range of cyber threats
  - Will be covered in Topic 2!
- Maintains trustworthiness, reliability, and accessibility of critical data and resources in organizations

AAA Model



- Identifying users trying to access a system through various means (facial recognition, MFA etc.)
- Ensures that only authorized parties are allowed to access
- We will learn more about authentication in Topic 3!

- Determines what actions an authenticated user is permitted to perform within the system
- Ensures that users can only access the resources and perform the actions that are appropriate for their role

- Tracking and logging of user activities and interactions within a system
- Provides a record of who accessed what resources, when, and what actions were taken

Access Control Measures

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role-Based / Rule-Based Access Control (RBAC)
- Segregation of Duties (SoD)
- Defense in Depth

Mandatory / Discretionary Access Control (MAC / DAC)

Mandatory Access Control (MAC)	Discretionary Access Control (DAC)
• Stricter access control than DAC • Access decisions are enforced based on specified rules and policies (may vary across organizations) • Access to resources is strictly controlled based on clearance levels and security classifications • Access to resources is often determined by a central authority / system administrator • More difficult to manage due to its rigid nature and organizations which adopt MAC often have many employees Examples where MAC is adopted: • Government agencies • Military organizations	• More flexible than MAC • Owners of resources can grant permissions to anyone at their own discretion to use their resources • Owners specify what actions each user can perform (CRUD: Create, Read, Update, Delete) Examples where DAC is adopted: • File systems in operating systems (Windows, macOS, Linux etc.)

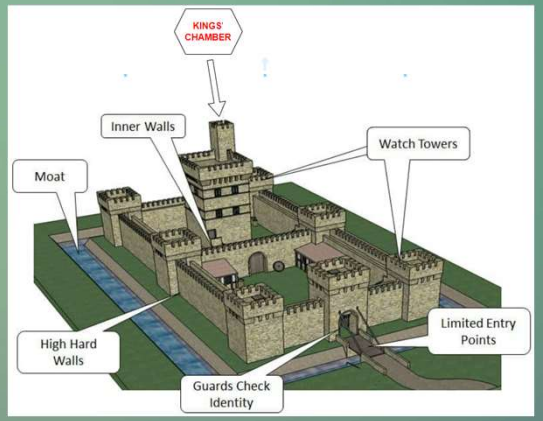
Role-Based / Rule-Based Access Control (RBAC)

ROLE-Based Access Control	RULE-Based Access Control
• Users are assigned permissions based on their roles within their organization • Users with similar roles will have similar privileges • Supports the principle of least privilege (where users are granted the minimal permissions to perform their jobs) • Not fixed as roles may differ on a case-by-case basis	• Users are assigned permissions based on specific conditions (e.g. user attributes, resource properties and environmental factors) • Conditions are stricter • Job titles are often ignored • More ideal for large organizations with many employees

Segregation of Duties (SoD)

- Dividing responsibilities among users
- No single user will have full control over a resource/process
- Prevents conflict of interest among users

Defense in Depth



- Imagine a castle with many layers of protection
  - Moat, Watch Towers, Limited Entry Points etc.
  - Why are so many layers needed?

- Defense in depth involves deployment of multiple layers of security
  - Includes firewalls, IDS, IPS, antivirus software etc.
    - Will be covered in Topic 6!
- Principle of Redundancy
  - Having more lines of defense ensures that if one control is bypassed, other controls provide backup protection

Topic 1 Summary

- Overview of Cybersecurity
- Common terms used in cybersecurity
- Various access control measures

In the next topic...

Understanding Cyber Threats

- Common cyber threats
- Phishing awareness
- Mitigating cyber threats