Cybersecurity

CS202 Lecture 24

Lecture Outline

Section 1: Introduction

1. **Definition** of Cybersecurity
2. **CIA Traid** (Confidentiality, Integrity, and Availability)
3. **Importance** of Cybersecurity
4. **Brief History** of Cybersecurity

Section 2: Threat Landscape

1. **Types of Threats:**
   - Malware (Viruses, Worms, Trojans)
   - Phishing and Social Engineering
   - Ransomware
   - Denial of Service (DoS) and Distributed Denial of Service (DDoS)
2. **Threat Actors:**
   - Script Kiddies
   - Hackers
   - Cybercriminals
   - Nation-State Actors
   - Insider Threats
3. **Common Attack Vectors:**
   - Email
   - Web
   - Network
   - IoT Devices

Lecture Outline

Section 3: Cybersecurity Fundamentals

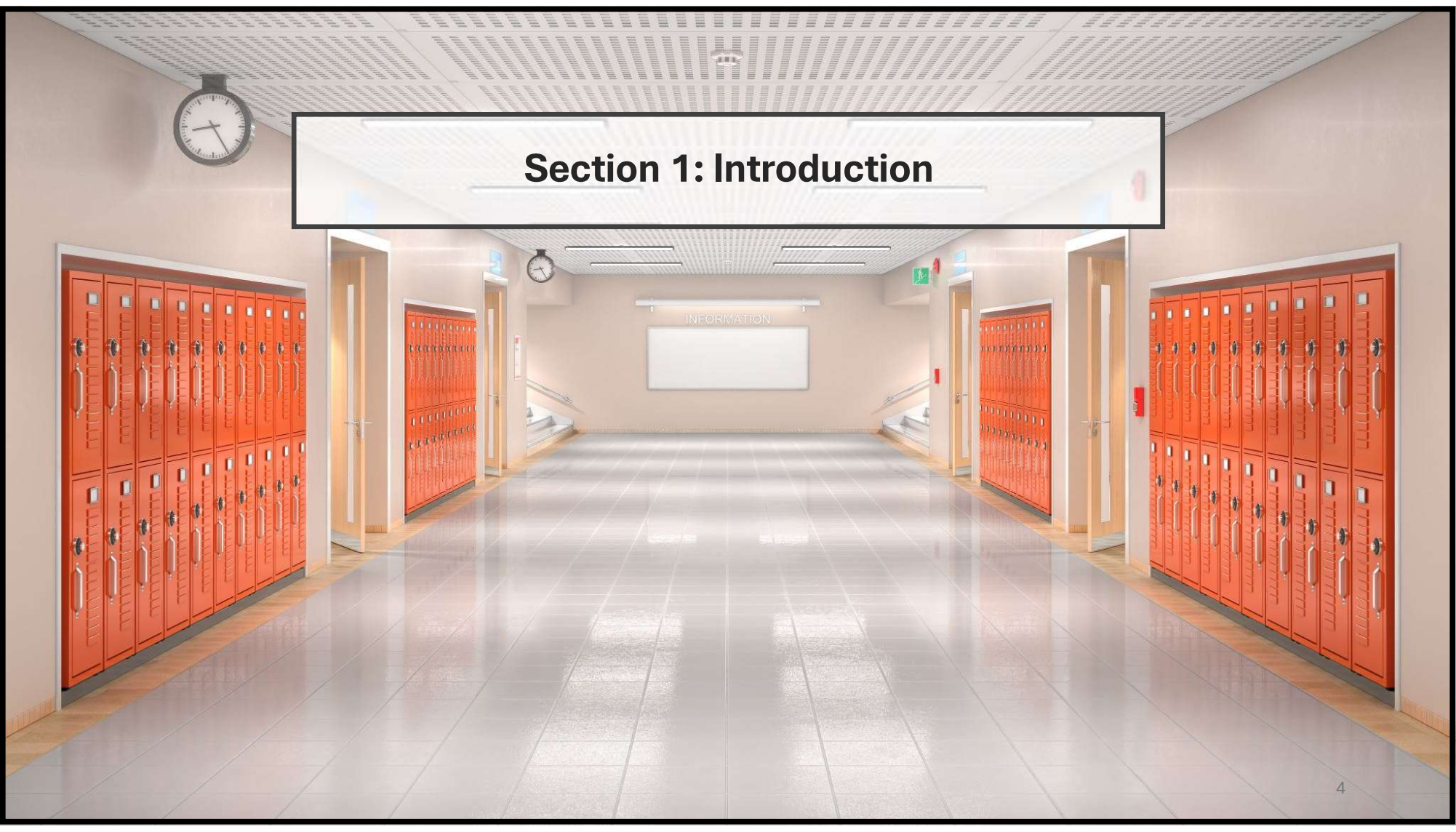
1. Authentication, Authorization, and Accounting (AAA)
2. Encryption: Types (symmetric, asymmetric), Uses (data at rest, data in transit)
3. Password management and password policies

Section 4: Security Controls and Measures

1. Firewalls and network segmentation
2. Intrusion Detection/Prevention Systems (IDS/IPS)
3. Endpoint security: Antivirus software, Endpoint Detection and Response (EDR)
4. Identity and Access Management (IAM)
5. Backup and disaster recovery

Section 5: Best Practices and Future Directions

1. Cybersecurity hygiene: Software updates, Patch management, Regular backups
2. Emerging trends: AI/ML, Cloud security, IoT security
3. Careers in cybersecurity


Section 1: Introduction
INFORMATION

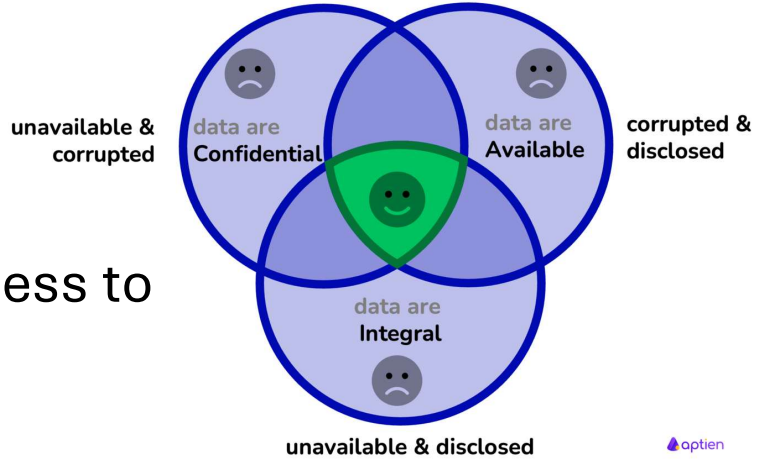
Definition of Cybersecurity

Introduction to Cybersecurity:

- Protecting systems, networks, and data from cyber threats

- Ensure:
  - Confidentiality
  - Integrity
  - Availability (CIA Triad)

CIA Triad



Confidentiality: Prevent unauthorized access to sensitive data

- Example: Encrypting sensitive files

Integrity: Protect data from unauthorized modifications

- Example: Using checksums to verify data accuracy

Availability: Ensure systems and data are accessible when needed

- Example: Implementing redundant systems and backups

Importance of Cybersecurity

Safeguards:

- Personal data (e.g., banking information)
- Critical infrastructure (e.g., power grids)
- Business operations (e.g., intellectual property)

Rising cyber threats:

- Cybercrime projected to cost $8 trillion globally in 2023
- Increasing dependence on digital systems

Brief History of Cybersecurity

1970s: First computer worm, 'Creeper', identified

1980s: Rise of antivirus software (e.g., Norton)

2000s: High-profile breaches (e.g., TJX hack in 2007)

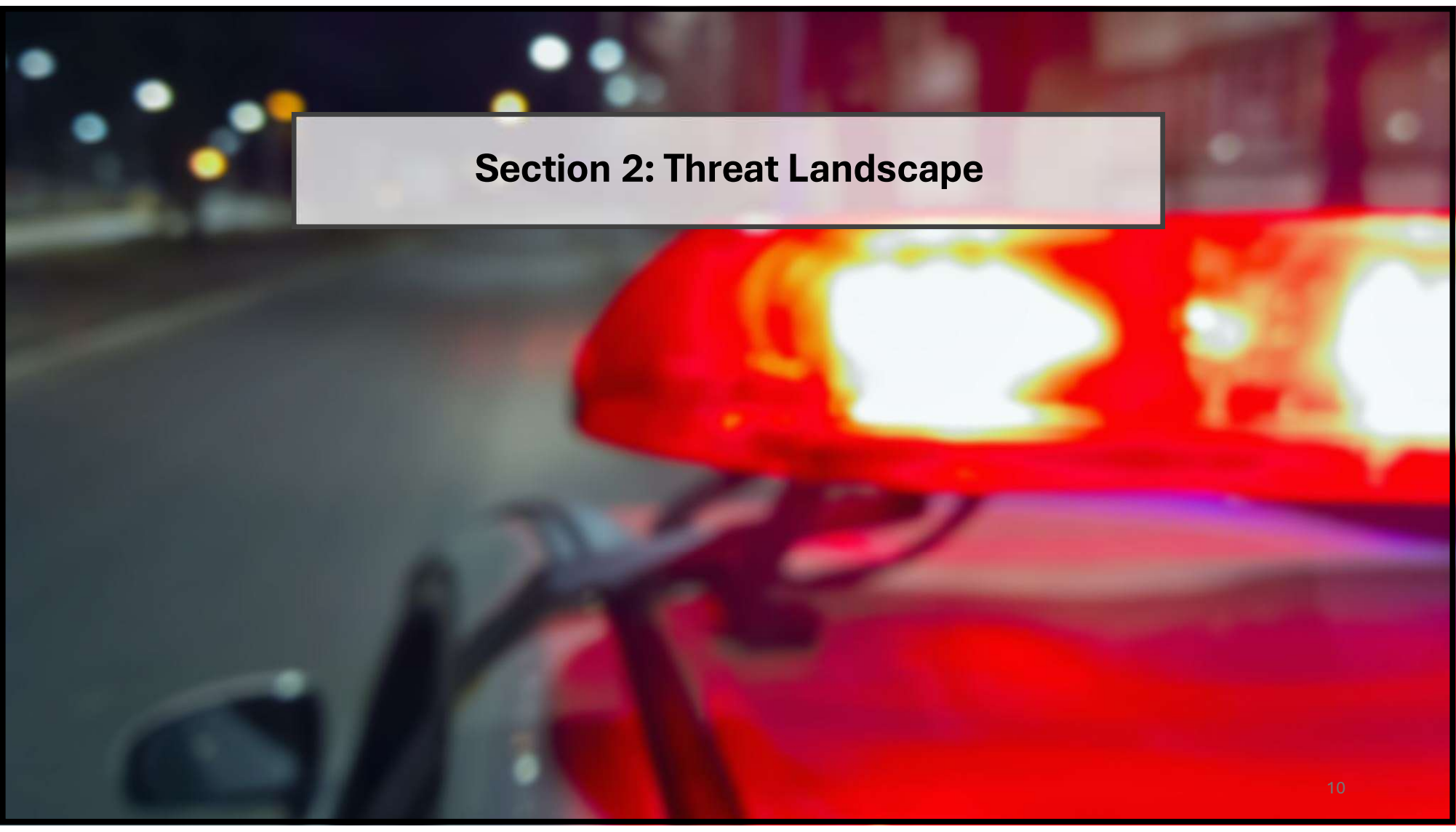
2010s–2020s:

- Ransomware surge (e.g., WannaCry 2017)
- Zero Trust Architecture gaining traction

Transition to the Next Section

- To summarize, cybersecurity is about safeguarding systems, data, and networks in an increasingly digital world.
- Its importance is underscored by the growing complexity and frequency of threats.

- Next, we'll dive deeper into the types of cyber threats and foundational principles for defense.


Section 2: Threat Landscape

Types of Threats – Malware

Malware: Malicious software designed to harm or exploit systems

- **Viruses:** Attach to legitimate files, spread when executed
- **Worms:** Self-replicating, spread without user action
- **Trojans:** Disguised as legitimate software to execute harmful actions

Types of Threats – Phishing and Social Engineering

Phishing: Deceptive emails/websites to steal sensitive information

Social Engineering: Manipulating people to reveal confidential data

Examples:

- Fake login pages
- Urgent messages asking for passwords

Types of Threats – Ransomware

Ransomware: Lock files or systems, and demand payment for decryption

High-profile example: WannaCry (2017)

Prevention:

- Regular backups
- Updated software and security patches

Types of Threats – DoS and DDoS

DoS: Overloads a system, making it unavailable

DDoS: Distributed version using multiple systems to attack simultaneously

Impact:

- Disrupts services
- Financial and reputational damage

Threat Actors – Overview

Threat Actors: Individuals or groups behind cyberattacks

Motivations:

- Financial gain
- Espionage
- Ideological reasons

Threat Actors – Script Kiddies

- **Inexperienced or low-skilled attackers** who rely on pre-made hacking tools, scripts, or software created by more advanced hackers
- They do **not** typically understand how the underlying attack works
- They simply run tools to cause disruption or gain unauthorized access
- Motivated mainly by **fun, curiosity, bragging rights, or mischief**
- Often target systems with **weak security**
- Considered **low-level threat actors**, but can still cause significant damage

- In short, script kiddies don't “hack” by themselves — they **run someone else’s hacks**

Threat Actors – Hackers

Categories based on Hacker's Intent:

- **White-hat:** Ethical hackers, work to improve security
- **Black-hat:** Malicious intent, exploit vulnerabilities
- **Grey-hat:** Operate in legal and illegal gray areas

Threat Actors – Cybercriminals

Cybercriminals: Organized groups focused on financial gain

Activities:

- Identity theft
- Credit card fraud
- Selling stolen data on the dark web

Threat Actors – Nation-State Actors

Nation-State Actors: Sponsored by governments

Goals:

- Espionage
- Disrupt rival nations

Example:

- Stuxnet worm targeting Iran's nuclear program

Threat Actors – Insider Threats

Insider Threats: Employees, contractors, or partners misusing access

Motivations:

- Financial gain
- Revenge
- Negligence

Mitigation:

- Access controls
- Monitoring

Common Attack Vectors – Overview

Attack Vectors: Entry points attackers use to compromise systems

Exploited through:

- Human error
- Weak configurations

Common Attack Vectors – Email

Methods:

- Phishing emails
- Malware attachments

Prevention:

- Email filtering
- User awareness training

Common Attack Vectors – Web

Risks:

- Malicious websites
- Drive-by downloads

Prevention:

- Browser security
- Regular updates

Common Attack Vectors – Network

Exploitation:

- Unsecured networks
- Poorly configured firewalls

Defense:

- Encryption
- Intrusion detection systems (IDS)

Common Attack Vectors – IoT Devices

Challenges:

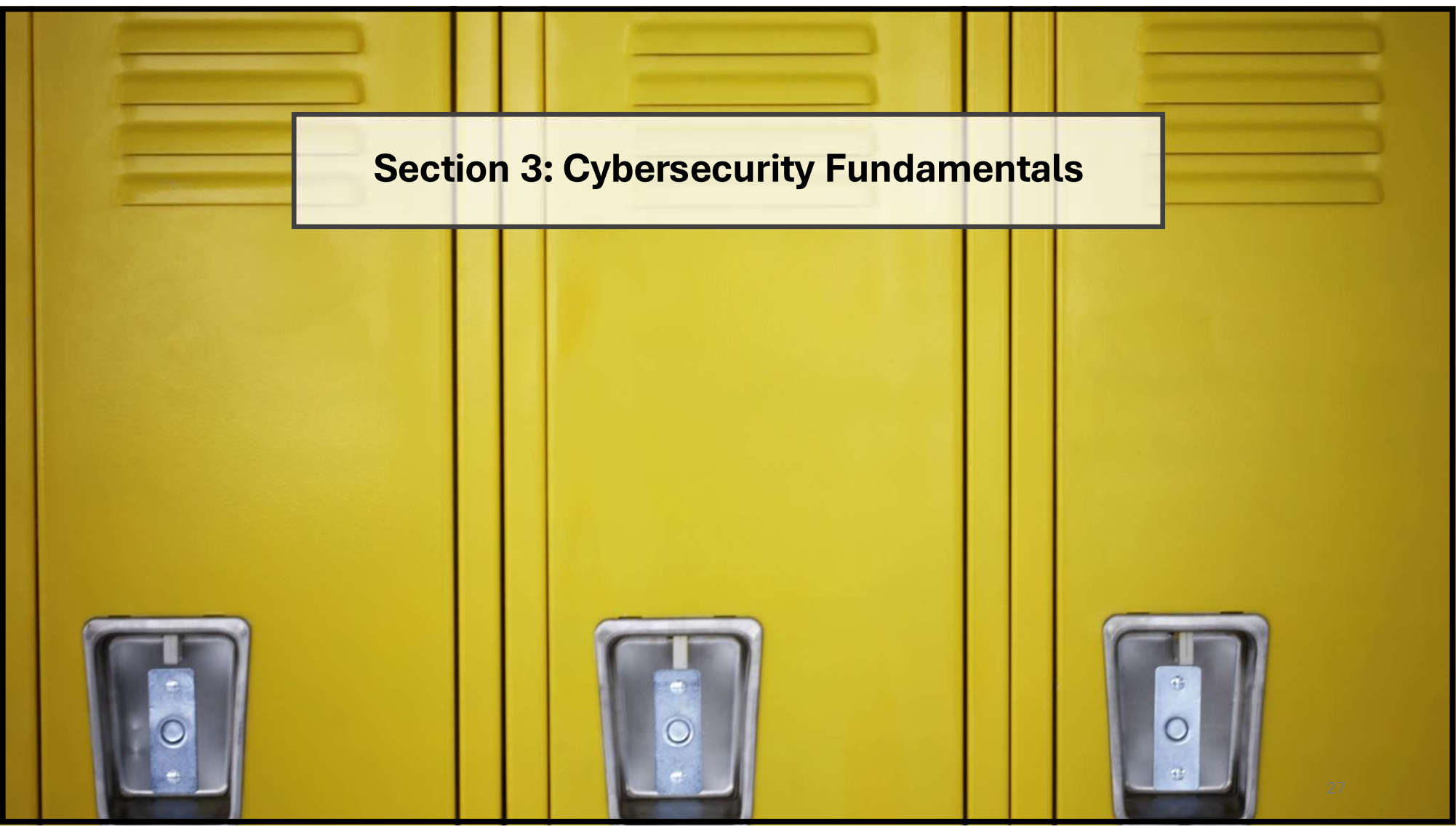
- Weak default security
- Lack of regular updates

Solutions:

- Strong device authentication
- Network segmentation

Transition to Next Section

- To summarize, we've explored various types of threats, the people behind them, and the common attack vectors.
- Next, we'll delve into the principles of cybersecurity and the strategies used to defend against these threats.


Section 3: Cybersecurity Fundamentals

Authentication, Authorization, and Accounting (AAA)

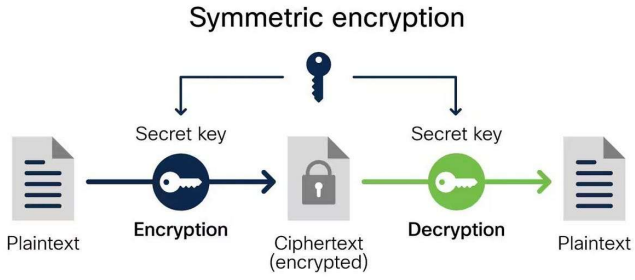
Authentication: Verifies user identity (e.g., passwords, biometrics)

Authorization: Grants permissions based on user roles

Accounting: Logs user activities for audits and compliance

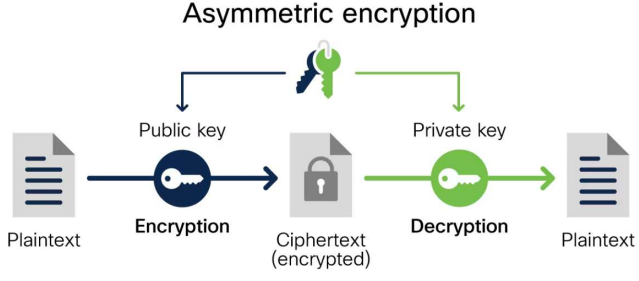
Encryption – Overview

Encryption: Protect data by converting it into unreadable formats



Key types:

- **Symmetric encryption:** Same key for encryption/decryption
- **Asymmetric encryption:** Public/private key pairs



Encryption – Use Cases

Data at rest:

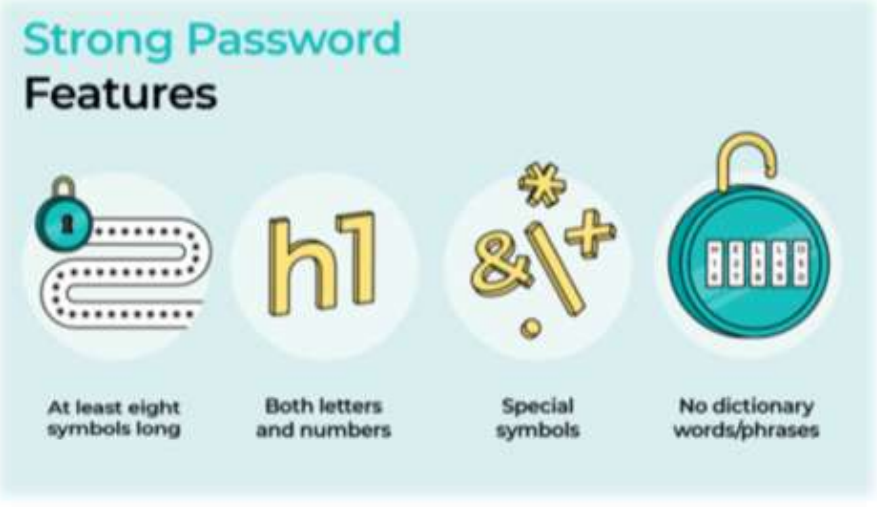
- Encrypt stored files and databases
- Example: BitLocker, database encryption

Data in transit:

- Secure communication
- Example: HTTPS, VPNs, email encryption

Password Management – Best Practices

- **Use strong passwords:**
  - Length > 12 characters
  - Include letters, numbers, and symbols
- **Avoid reusing passwords**
- **Use a password manager for secure storage**



Password Policies

Enforce:

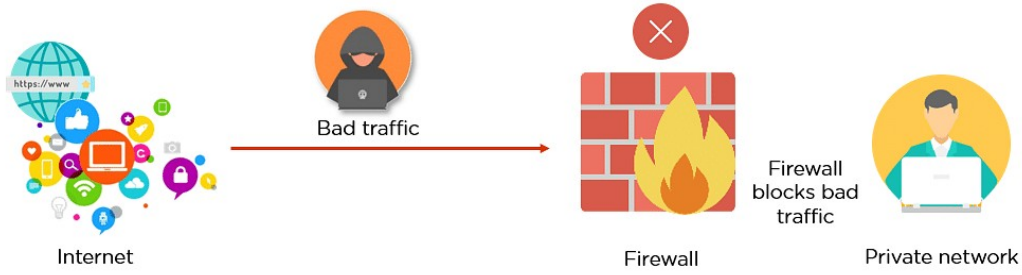
- Regular password changes
- Complexity requirements

Educate:

- Avoid writing down passwords
- Recognize phishing attempts targeting credentials

Section 4: Security Controls and Measures

What is Firewall?



Firewall:

- First line of defence for networks
- Barrier between trusted and untrusted networks

Types:

- Packet filtering
- Stateful inspection
- Next-Generation Firewalls (NGFW)

Functions:

- Block unauthorized access
- Monitor traffic for malicious activity

Next-Generation Firewalls

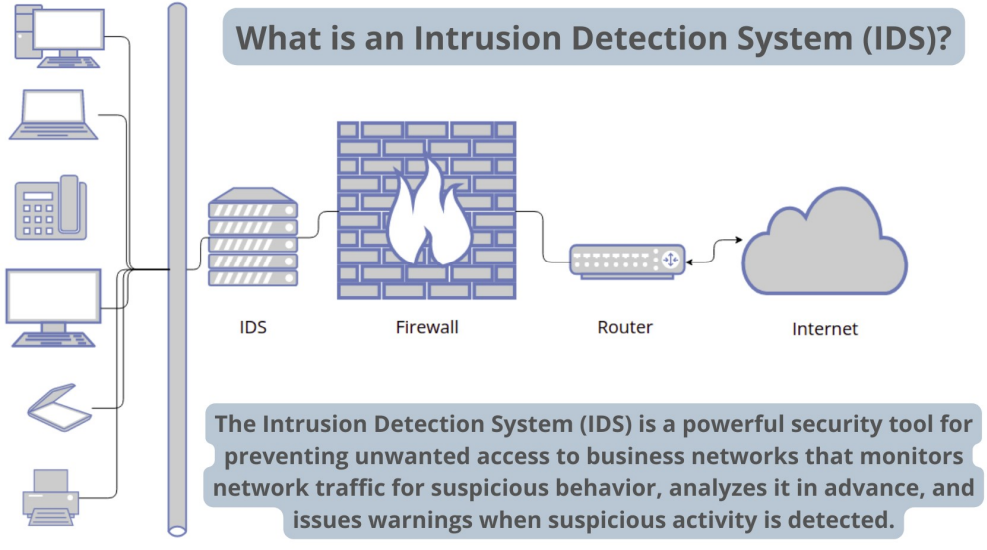
The next-generation firewall is a security device that combines a number of functions of other firewalls. It incorporates packet, stateful, and deep packet inspection.

Key Features of Firewalls

1. **Packet Filtering:** Analyzes data packets against rules to block/allow traffic
2. **Stateful Inspection:** Tracks active connections to ensure legitimate communication
3. **Proxy Functionality:** Acts as an intermediary, masking internal network details
4. **Network Address Translation (NAT):** Conceals private IPs by translating them into a public address
5. **Intrusion Prevention System (IPS) Integration:** Detects and blocks threats in real time

What is an Intrusion Detection System (IDS)?

- **Definition:** A system that monitors network traffic for suspicious activity or known threats
- **Types:**
  - Host-Based IDS (HIDS)
  - Network-Based IDS (NIDS)
- **Purpose:**
  - Detect intrusions and alert administrators
  - Enhance network visibility



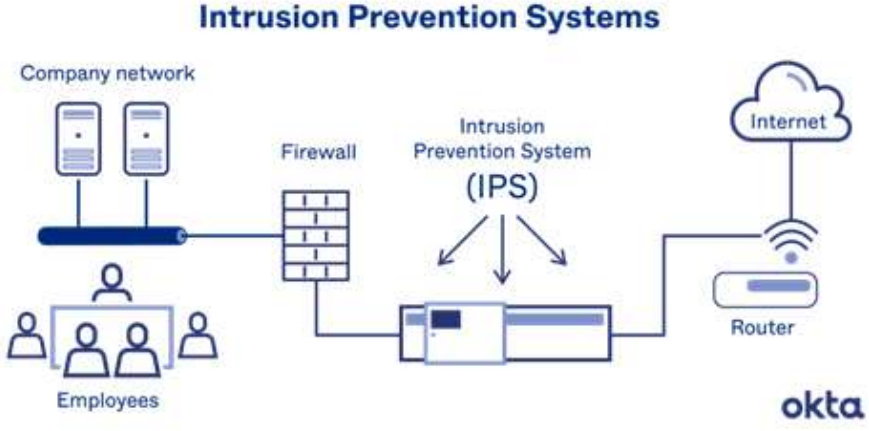
Network Security – Intrusion Detection and Prevention Systems (IDS/IPS)

IDS: Monitors traffic for malicious activity

- **Types:** Signature-based, anomaly-based

IPS: Automatically blocks detected threats

- **Example:** Blocking known attack patterns



Differences: Firewall vs. IDS

Feature	Firewall	Intrusion Detection System (IDS)
Primary Goal	Regulate access to ensure secure traffic.	Detect malicious activity or threats.
Functionality	Filters and blocks unauthorized traffic.	Monitors traffic for anomalies.
Operation	Real-time filtering based on rules.	Real-time or log-based analysis.
Response	Proactively blocks threats.	Generates alerts for investigation.
Placement	Perimeter of the network.	Within the network near critical assets.

Summary

Concept	Purpose
Confidentiality	Keep data private
Integrity	Prevent tampering
Availability	Ensure access
Authentication	Verify identity
Authorization	Grant permissions
Encryption	Secure data
Malware	Understand threats
Firewalls	Protect networks
Vulnerabilities	Fix weaknesses
Social Engineering	Prevent human-targeted attacks


The End.