CSC 116: Overeview

Definition of Cybersecurity

Cybersecurity is the practice of protecting systems, networks, devices, and data from cyber threats, unauthorized access, and malicious attacks. It involves implementing technologies, processes, and practices designed to safeguard sensitive information and ensure the confidentiality, integrity, and availability of digital assets.

Cybersecurity covers various domains, including:

1. **Network Security:** Protecting computer networks from intrusions, attacks, and misuse.
2. **Information Security:** Ensuring the confidentiality, integrity, and availability of data.
3. **IOT Security:** Securing devices such as computers, smartphones, and other connected small devices.
4. **Application Security:** Safeguarding software applications from vulnerabilities and unauthorized access.
5. **Operational Security:** Managing processes and decisions related to protecting data and assets.
6. **Cloud Security:** Securing cloud computing environments, including data storage and applications.
7. **Identity and Access Management (IAM):** Controlling user access and authentication to sensitive resources.
8. **Access Control**

Security & Privacy

Security

Definition: **Security refers to the state or condition of being protected from or not exposed to harm, danger, or unauthorized access**. It encompasses measures, policies, and practices designed to safeguard assets—whether physical, digital, or organizational—from threats and vulnerabilities.

What is the difference between privacy?

Security

Attack
Your
Phone

Information Privacy

Stealing Your Information

1 **Installing a surveillance camera** in a building to monitor and prevent unauthorized access.
(Focus: Protecting the physical space.)

2 **Sharing your location** with an app.
(Focus: Controlling personal data usage.)

3 **Refusing to allow a social media platform** to collect browsing history for targeted ads.
(Focus: Protecting user preferences.)

4 **Using a firewall** to prevent unauthorized access to a computer network.
(Focus: Safeguarding digital systems.)

5 Deleting personal data (e.g., address, phone number) from a public directory.
(Focus: Limiting access to personal information.)

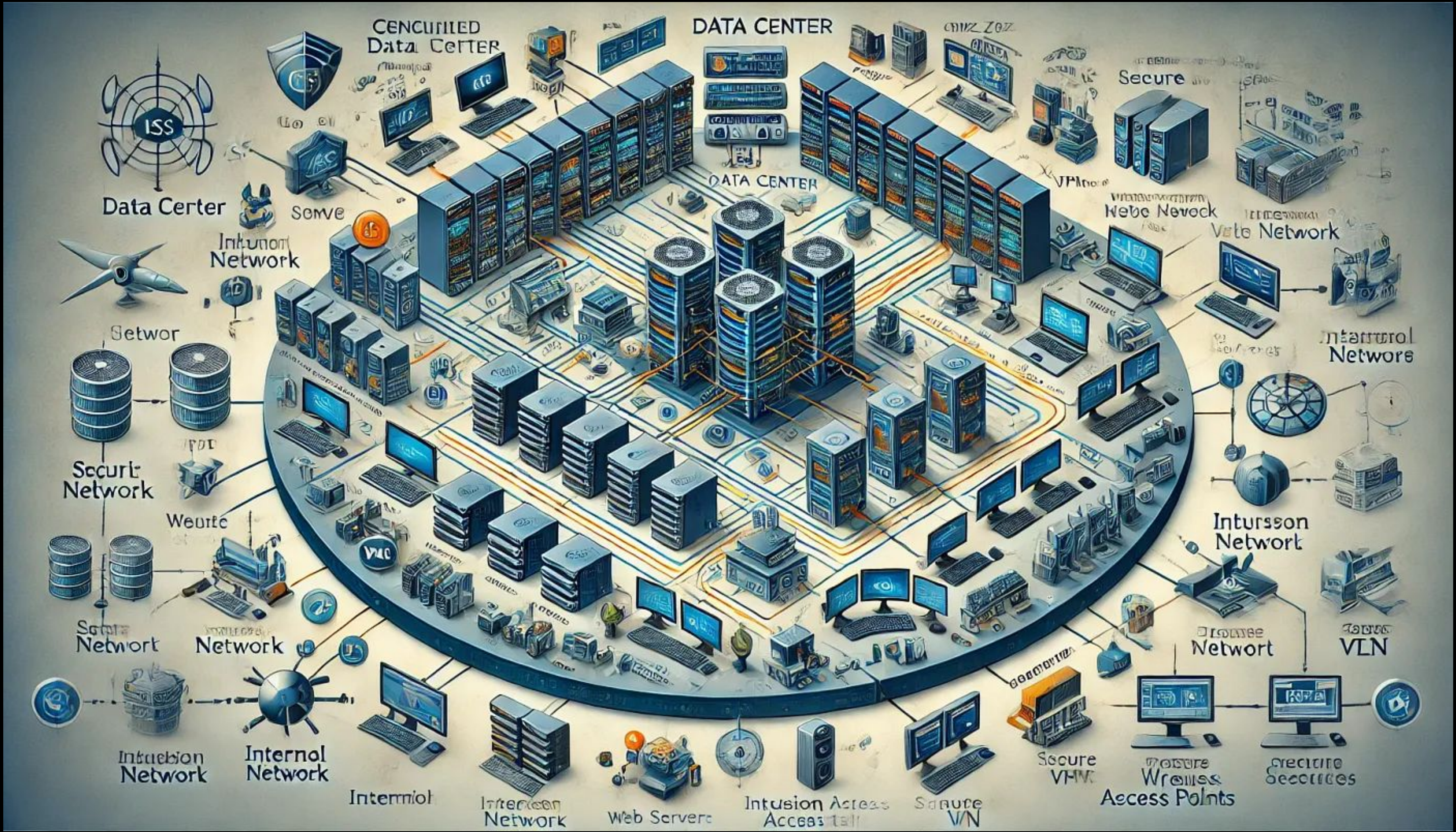
6 Using an anonymous ID in a forum.
(Focus: Protecting identity.)

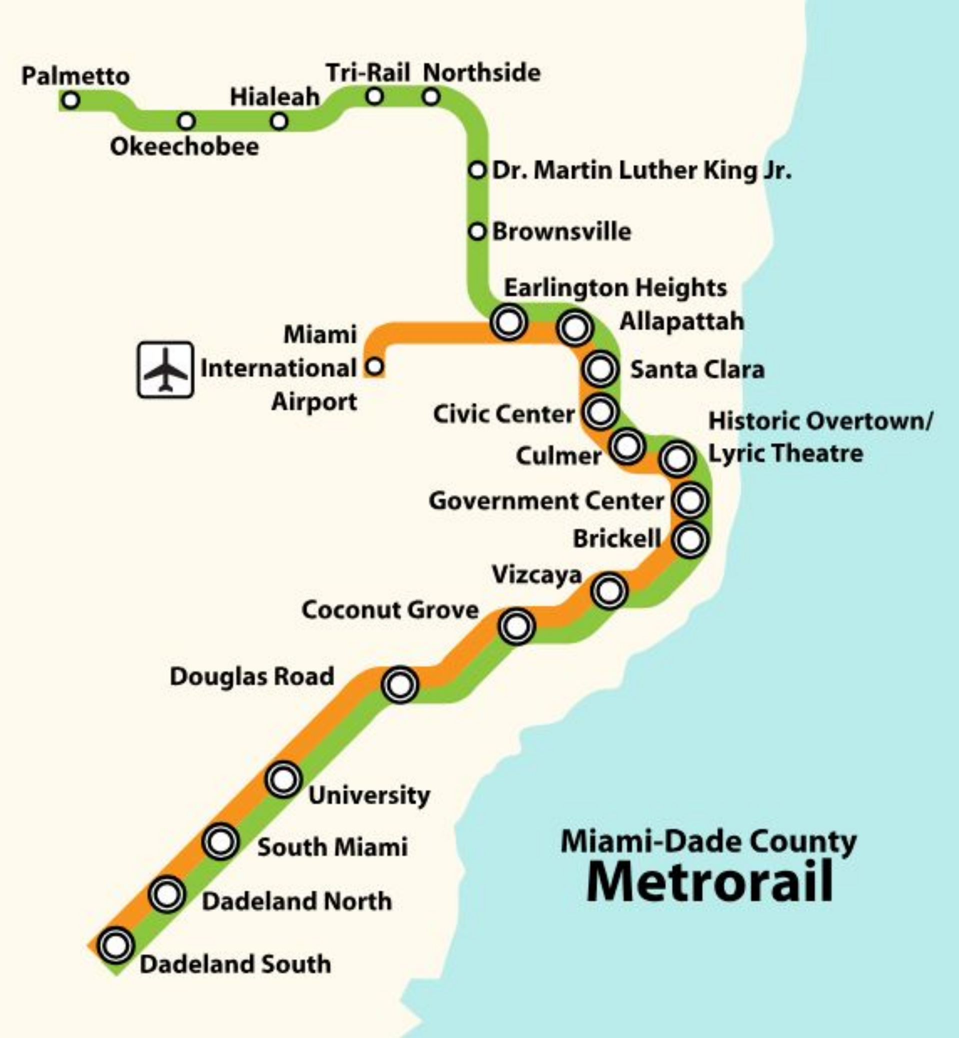
7 Hiring security guards to patrol a sensitive area.
(Focus: Protecting physical assets.)

8 Encrypting communications between devices to prevent eavesdropping.
(Focus: Securing data during transmission.)

9 Implementing multi-factor authentication for accessing sensitive systems.
(Focus: Verifying identity to protect resources.)

Network Security


CENCUIILED
Data Certer
DATA CENTER
Secure
ISS
Data Certer
Sewe
DATA CENTER
VPN
Webe Nevock
Vete Network
Intruion
Network
Setwor
Intarnurol
Networe
Securt
Network
Weurte
Intursson
Network
Network
Network
Network
VLN
Intuebion
Network
Internol
Network
Internioi
Intercon
Network
Web Server
Intusion Actess
Accestal
Secure
VHN
Senure
VN
Wreless
Acess Points
Secorices


Palmetto
Okeechobee
Hialeah
Tri-Rail
Northside
Dr. Martin Luther King Jr.
Brownsville
Earlington Heights
Allapattah
Miami
International
Airport
Santa Clara
Civic Center
Culmer
Historic Overtown/
Lyric Theatre
Government Center
Brickell
Vizcaya
Coconut Grove
Douglas Road
University
South Miami
Dadeland North
Dadeland South
Miami-Dade County
Metrorail

Questions:
Any security problems in the network?

1. Security Problems
2. Privacy
3. Network Delay
4. Server Crash, no services (**no avaliability**),
if the server is being attacked (**no safety**),
the server sometimes works,sometimes not,
and it takes long time to get the data (no
liveness)

Availability refers to the system’s ability to respond to requests and provide service. A system with high availability can reliably handle operations without interruptions, ensuring that users can access resources when needed.

Safety means that the system operates in a manner that prevents undesirable outcomes. It guarantees that the system doesn’t enter an incorrect or harmful state, ensuring data integrity and protection against invalid or unauthorized actions.

Liveness involves the system’s capability to eventually make progress. A system is said to have liveness if it can continue executing tasks and eventually reach a desirable state, rather than being stuck in a non-responsive or waiting condition indefinitely.

Internet of the Things

Defintions: The **Internet of Things (IoT)** refers to a network of physical devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data.

IoT devices—also known as “smart objects”—can range from simple “smart home” devices like smart cameras, to wearables like smartwatches to complex industrial machinery and transportation systems. Technologists are even envisioning entire “smart cities” predicated on IoT technologies.

IoT camera vulnerability:
An attacker exploits a known vulnerability in a network camera's firmware, remotely accessing the device to view private video streams. This can occur due to weak default passwords or unpatched firmware.

Phishing attack on an employee's laptop:
In an enterprise setting, a laptop is considered an endpoint. If an employee clicks a malicious link in a phishing email, an attacker may inject malware that uses the laptop as a gateway to infect the company's internal network.

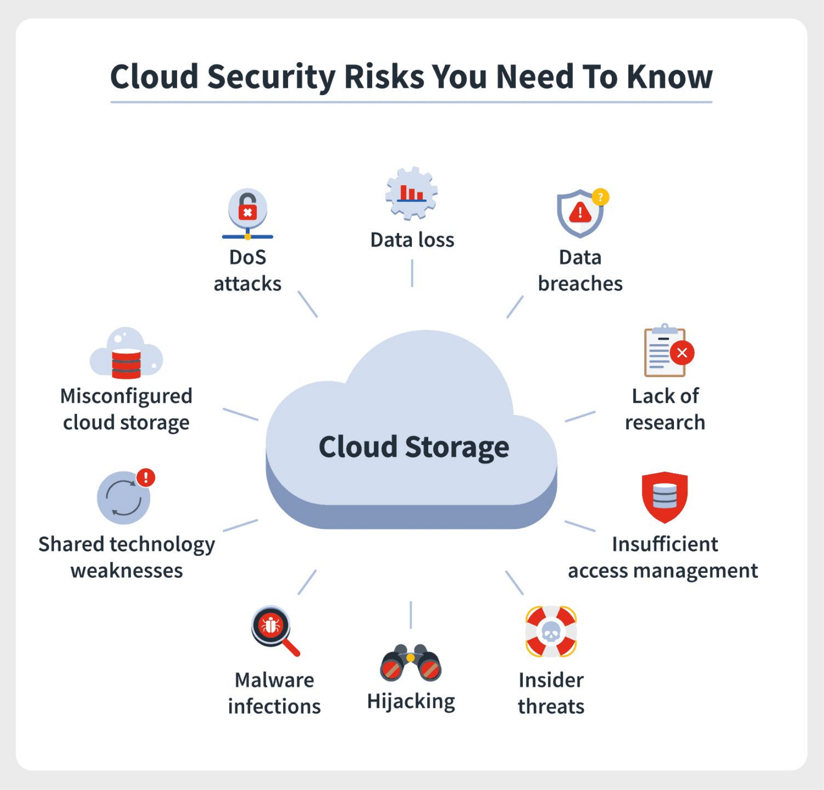
Unencrypted IoT device communications:
Some IoT devices communicate without encryption. Attackers intercept network traffic to capture sensitive information, such as unlock commands for a smart home door lock.

Application Security

Application security: refers to the process of identifying, mitigating, and preventing vulnerabilities and threats within software applications. It encompasses various tools, techniques, and practices designed to protect an application’s data, functionality, and underlying systems from unauthorized access, data breaches, and other malicious activities.

Cloud Security

https://aws.amazon.com/
https://cloud.google.com/


Cloud Security Risks You Need To Know
Cloud Storage
DoS attacks
Data loss
Data breaches
Misconfigured cloud storage
Lack of research
Shared technology weaknesses
Insufficient access management
Malware infections
Hijacking
Insider threats

https://www.coursera.org/learn/aws-infrastructure-security

Access Control

Access control is a security measure that restricts who can view or use resources in a system. It ensures only authorized users, devices, or applications can access certain data or functions. Key steps include identifying users, verifying their credentials, and granting permissions based on their role or clearance level. This helps protect sensitive information and prevent unauthorized activities.

Identity Management

Identity and Access Management (IAM)

Identity and Access Management (IAM) is a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay.