CSC 116 Overview

Instructor: Yusen Wu, PhD

Department of Neurology,
Department of Computer Science,
Frost Institute for Data Science and Computing,
University of Miami

Would You Prefer to Do the Assignment Individually or in a Group?

by Yusen Wu · 1 day ago

Yes, I prefer to work in a group, I need team members to help me. 61.76% (21 votes)

No, each person should do the assignment independently 38.24% (13 votes)

Total votes: 34

Live results

Back to poll

Share

Find your group members: 1-3 students a group

Register your Group here!

Group

Cryptography

What is Cryptography?

- Think of it like **locking your diary** so no one else can read it.
- **Encryption = Locking** the information.
- **Decryption = Unlocking** it with the right key.
- Goal: **Keep data private, unmodified, and ensure the right person is using it.**

Three Core Functions of Cryptography

1. **Confidentiality (Encryption)**:
   Like putting a prescription in a sealed envelope.

2. **Integrity (No Tampering)**:
   - Making sure no one secretly changes the medication name.

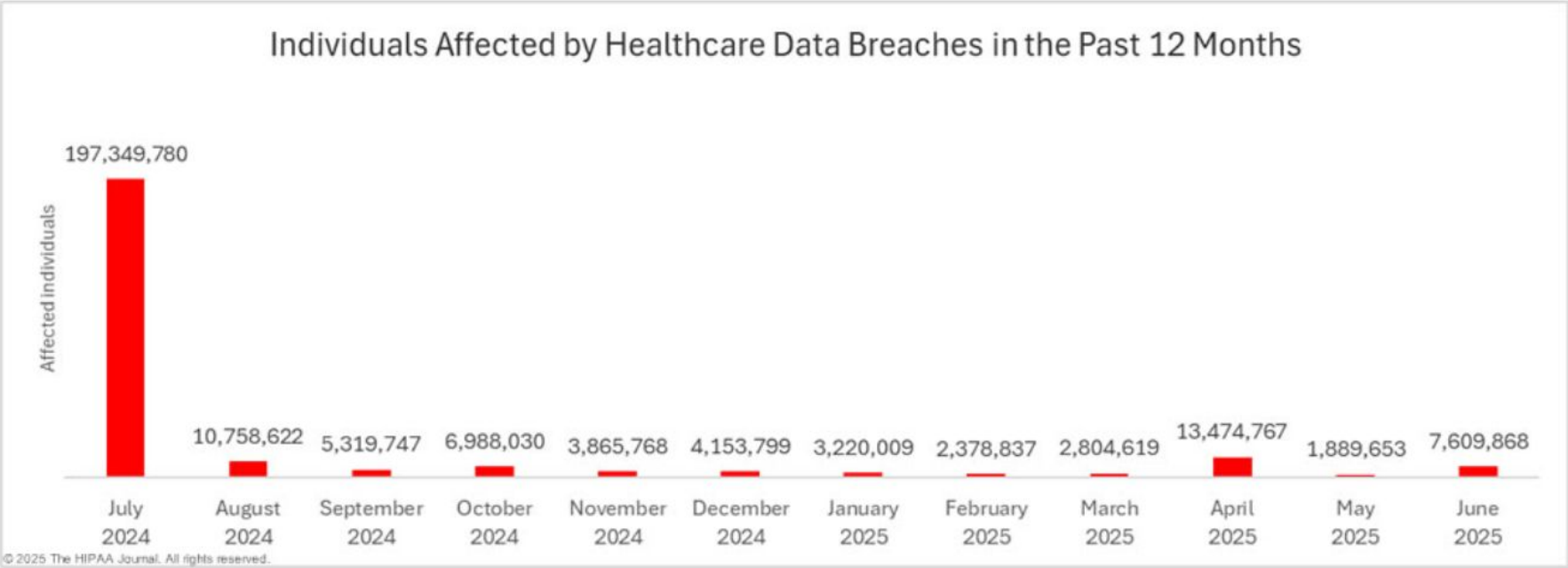
3. **Authentication (Identity Check)**:
   - Confirming the prescription really comes from the doctor, not an imposter.

Healthcare data is considered **highly sensitive** due to the nature of the information it contains and the potential negative consequences if it is compromised.

Here's why and what's included:

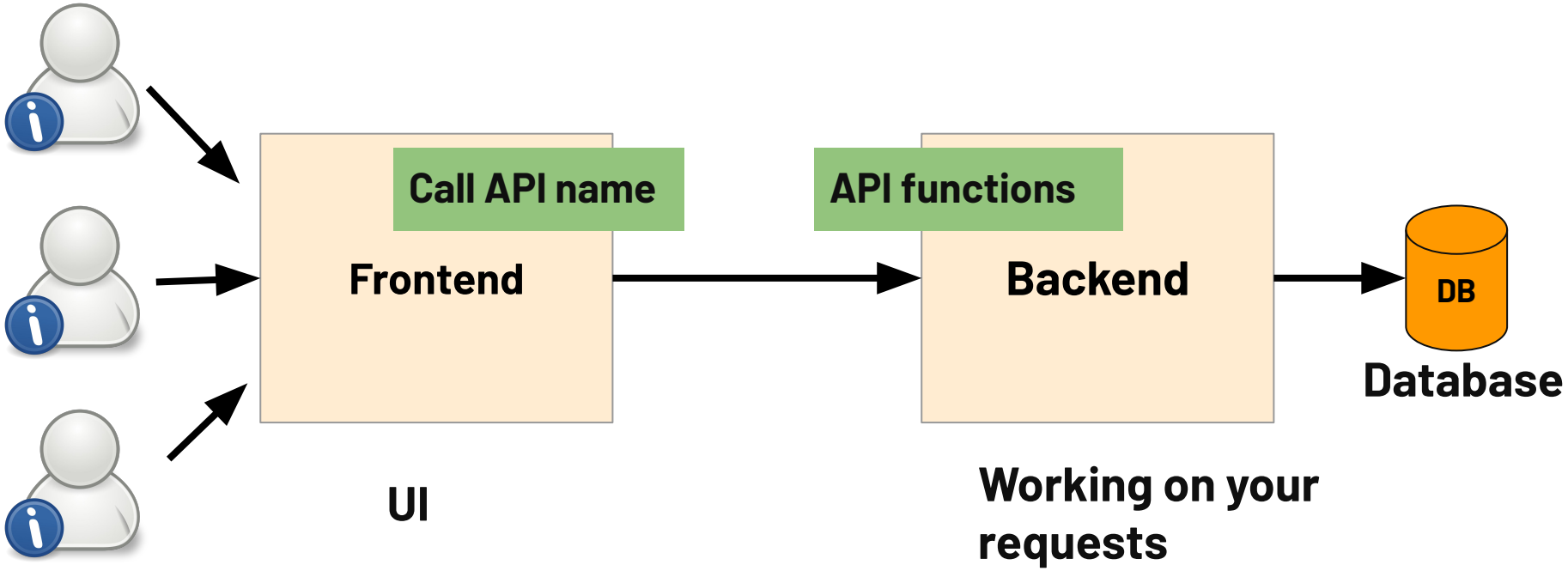
Why it's highly sensitive

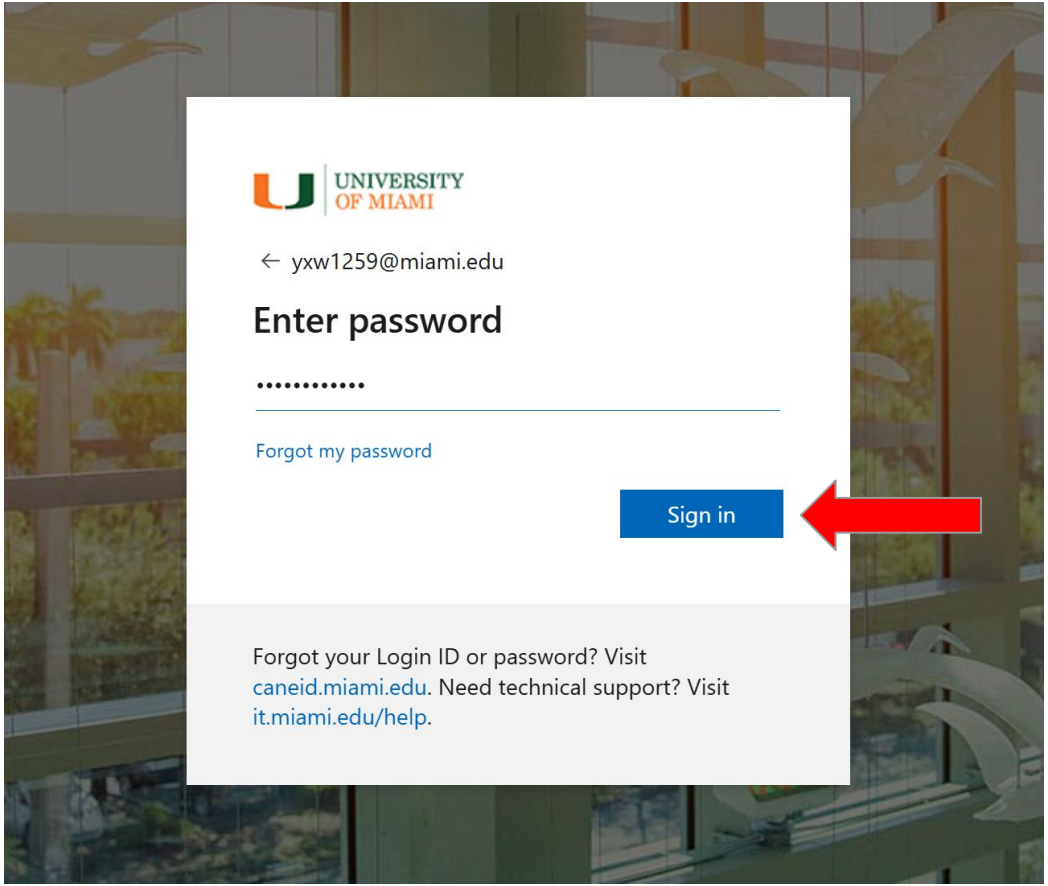
- Deeply personal information: Healthcare data includes a comprehensive record of a person's physical and mental health history, treatments, diagnoses, and personal identifying information (PII) like names, addresses, Social Security numbers, and dates of birth.
- Potential for exploitation: If compromised, this data can be used for identity theft, fraud (including insurance fraud), blackmail, or other malicious activities.

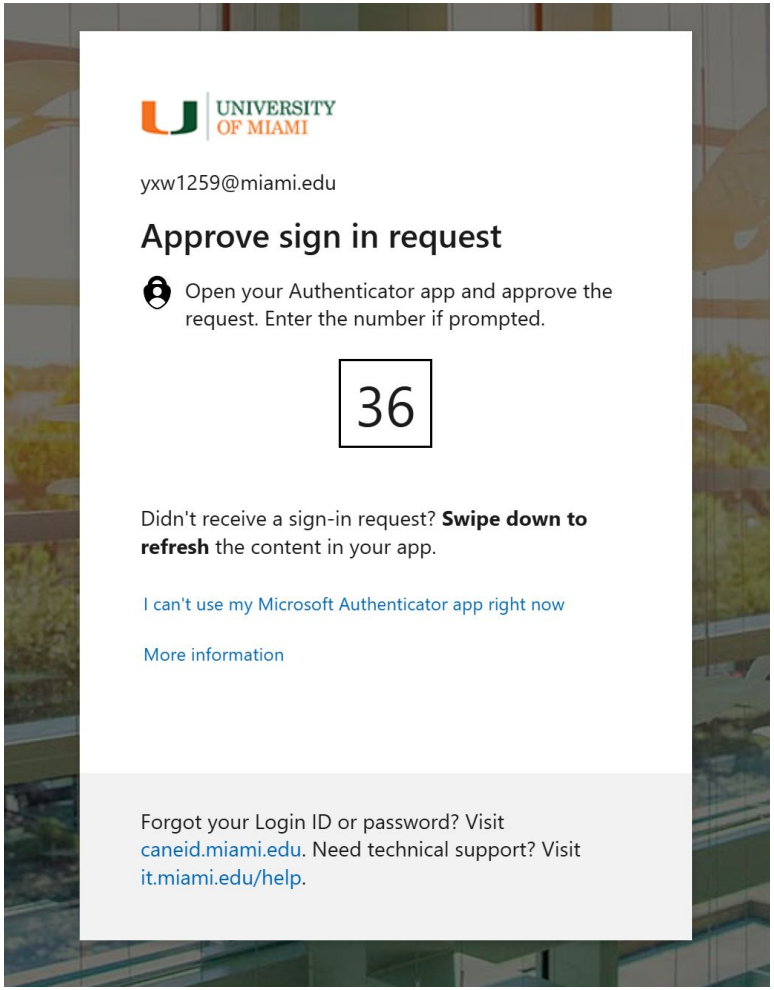

Individuals Affected by Healthcare Data Breaches in the Past 12 Months
Affected individuals
197,349,780
10,758,622
5,319,747
6,988,030
3,865,768
4,153,799
3,220,009
2,378,837
2,804,619
13,474,767
1,889,653
7,609,868
July 2024
August 2024
September 2024
October 2024
November 2024
December 2024
January 2025
February 2025
March 2025
April 2025
May 2025
June 2025
© 2025 The HIPAA Journal. All rights reserved.

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Cause of Breach
Episource, LLC	CA	Business Associate	5,418,866	Hacking incident – Data theft confirmed
McLaren Health Care	MI	Healthcare Provider	743,131	Ransomware attack – Data theft confirmed
Compumedics USA, Inc.	NC	Business Associate	318,150	Hacking incident – Data theft confirmed
Central Kentucky Radiology	KY	Healthcare Provider	166,953	Ransomware attack – Data theft confirmed
Southern Connecticut Vascular Center, LLC	CT	Healthcare Provider	154,417	Hacking incident
Select Medical Holdings Corporation	PA	Healthcare Provider	119,525	Hacking incident at business associate (Nationwide Recovery Service)
Horizon Healthcare RCM	IN	Healthcare Clearing House	77,410	Ransomware attack – Data theft confirmed
TRG, LLC	OR	Healthcare Provider	70,434	Hacking incident at business associate (Nationwide

System Architecture


Call API name
Frontend
API functions
Backend
DB
Database
UI
Working on your requests


UNIVERSITY OF MIAMI
yxw1259@miami.edu
Enter password
Forgot my password
Sign in
Forgot your Login ID or password? Visit caneid.miami.edu. Need technical support? Visit it.miami.edu/help.



we already have passwords why still need authentication?

Security and Privacy

Security

Definition: **Security refers to the state or condition of being protected from or not exposed to harm, danger, or unauthorized access.**

What is the difference between privacy?

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

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

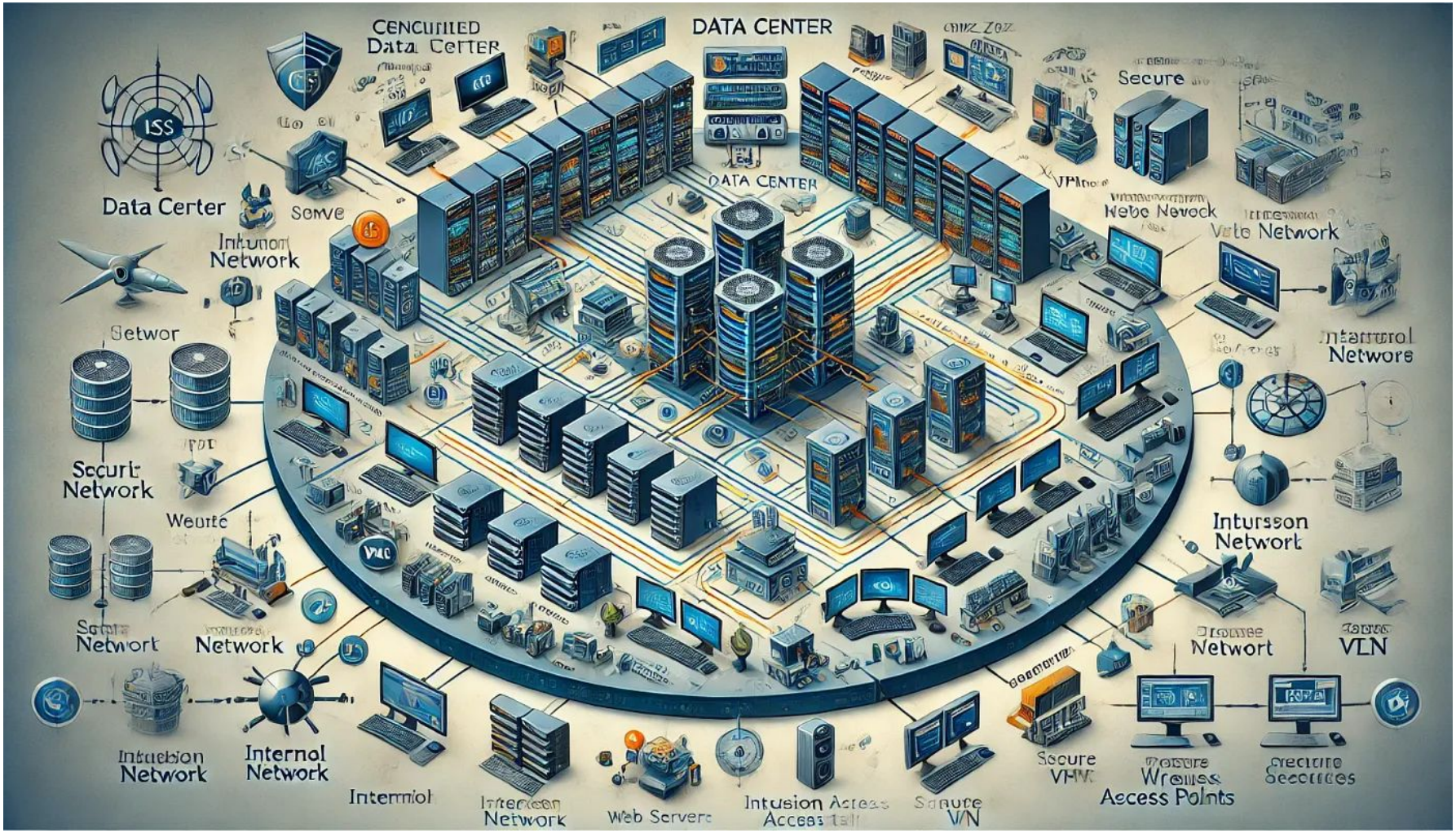
Security

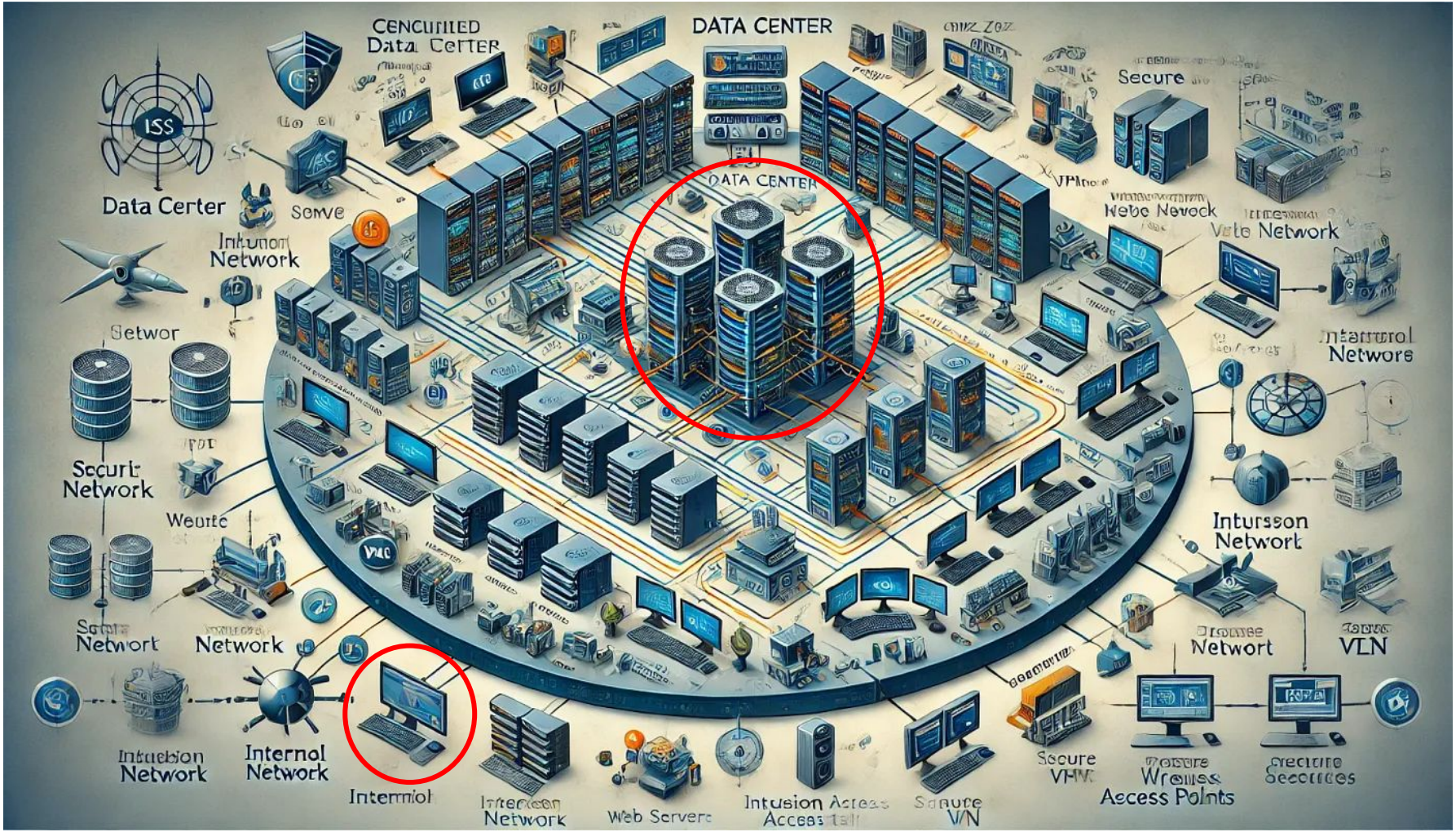
Attack

Privacy

Stealing Your Information

Network Security


CENCURIIED
DATA CERTER
DATA CENTER
ISS
Data Center
Serve
DATA CENTER
Secure
VPN
Webe Nevock
Veto Network
Intuion
Network
Setwor
Interurol
Networe
Securt
Network
Weurte
Intursson
Network
Network
Network
Network
VLN
Intruebion
Network
Internal
Network
Internoi
Intrucion
Network
Web Server
Intusion Access
Access
Sanure
VPN
Secure
VPN
Wreless
Access Points
Secorrees


DATA CENTER
Data Center
Secure
Network
Network
Network
Network
Internal
Network
Intrusion
Network
Secure
VLN
Secure
Access Points


Palmetto
Okeechobee
Hialeah
Tri-Rail
Northside
Dr. Martin Luther King Jr.
Brownsville
Earlington Heights
Allapattah
Miami International Airport
Santa Clara
Civic Center
Historic Overtown/ Lyric Theatre
Culmer
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. Data Privacy
2. Network Delay
3. 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)**

Questions:

Access UM website is ok because the website open sourced to everyone,

But if it is your salary?

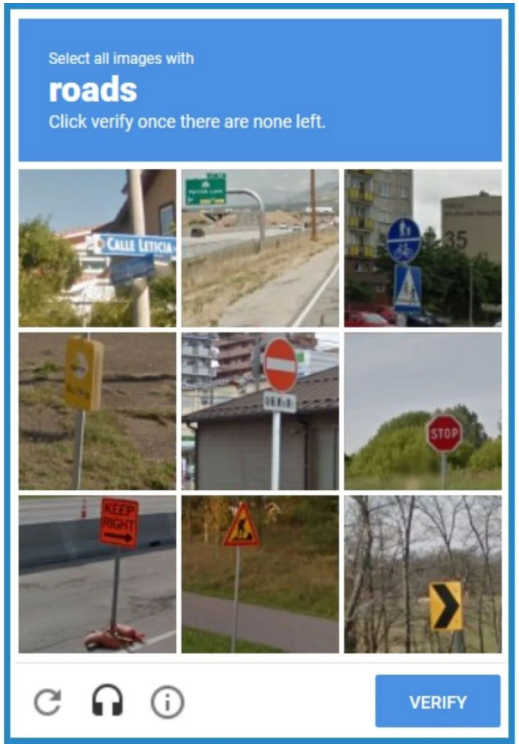
HyperText Transfer Protocol

http

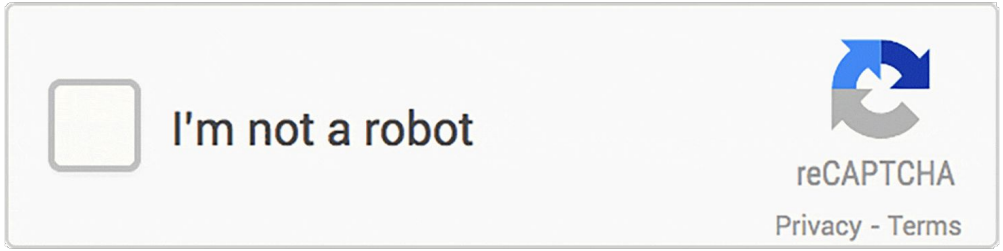
HyperText Transfer Protocol Secure

https

Feature	HTTP	HTTPS
Full Name	HyperText Transfer Protocol	HyperText Transfer Protocol Secure
Security	Plain text transmission — data can be intercepted, read, or modified	Encrypted with **TLS/SSL** — protects confidentiality and integrity
Certificates	No certificate required	Requires an **SSL/TLS certificate** (e.g., free from Let's Encrypt)
Performance	Slightly faster (no encryption overhead)	Slightly slower (due to encryption/decryption), but negligible with modern hardware
Browser Warning	Marked as **Not Secure** (especially for logins or payments)	Marked as **Secure** (padlock icon, "Secure" label)
Typical Use Cases	Testing, internal networks, non-sensitive info	Logins, payments, personal data, banking, healthcare, payroll — **any sensitive data must use HTTPS**


Select all images with
roads
Click verify once there are none left.
CALLE LETICIA
STOP
KEEP RIGHT
VERIFY

Question？


I'm not a robot
reCAPTCHA
Privacy - Terms

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. （!404）

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 (IoTs)

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.

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.

Cloud Security

https://aws.amazon.com/

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

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.

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.

https://www.youtube.com/watch?v=uqX1Qnt0IyY