# CS 3214
# Computer Systems

Cyber Security

Godmar Back

# Cybersecurity Concepts

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity
- Assurance

# Confidentiality

- Limit access to information to authorized parties
  - Privacy
- Threat: Interception
- Related to AAA:
  - Authentication
  - Authorization
  - Access Enforcement

# Integrity

- Ensure that unauthorized parties do not delete or modify data
  - Or authorized parties in a manner they are not authorized to do
- Threat: Modification

# Availability

- Ensure that information remains accessible, access control mechanisms are working in the intended way
- Threat: Interruption

# Authenticity

- Applied to data:
  - verifying the true origin of data and/or information
- Applied to users:
  - Assuring that users are who they say they are
- Threat: Fabrication
- Related to
  - Authentication: process of verifying information/data or users

# Anonymity

- Keeping the true identity of a principal secret
- Threat: Identification
- Not to be confused with Confidentiality/Privacy

# Assurance

- Part of Information Assurance
- Typically refers to processes, procedures, and mechanisms in place to uphold cybersecurity goals (CIA) and manage associated risks

# Web Applications

- Cybersecurity threats arise in the context of web applications; will discuss some of them

# Transport Layer Security

- SSL (past)/TLS family of protocols
  - Address confidentiality, integrity & authentication
- Threat of interception & impersonation
- Mitigation: Encryption & Attestation
- Layered protocol
  - Defends against MiM attacks
  - Also verifies identity of the server to client through certificates
  - See [Arnbak 2014] for challenges

# Configuring SSL/TLS

- Most web servers can be configured to enable SSL/TLS in a way that's mostly transparent to the remainder of the server
- Configuring SSL/TLS involves lots of trade-offs, best practices regarding cipher choice and legacy support are shifting; see https://www.ssllabs.com/ssltest/ for some example
- SSL Termination
  - Use SSL/TLS to gateway and use (faster) http unencrypted in intranet.

# Authentication Methods

- Different authentication methods:
  - Passwords, Biometric, 2FA, etc.
- Carrying authentication information:
  - Authentication headers
  - Cookies
- Stateful vs. stateless authentication
  - How does server remember previous authentication?
- Separation of resource servers & identity providers

# Identity Providers

- Many systems allow moving authentication to a central service and provide protocols for resource providers to have users authenticated using such services
- Examples:
  - Oauth (Google, FB, GitHub, etc.)
  - CAS (University Service)
- Example: Oauth workflow [1]

# JWT

- Claims:
  - Things that the holder of the token claims
  - E.g.: I am ... (insert subject here) and I have authenticated (insert iat here) which should be valid until (insert exp) here.
- Example: jwt.io

# JWT – Digital Signatures

- JWT can be signed and, optionally, encrypted.
  - (In project, JWT are not encrypted – thus, do not store confidential information in them.)
- Digital Signature through HMAC
  - Hash-Based Message Authentication Code [1]
- Ensures that payload has not been tempered with
  - If private key is used, also allows 3rd parties to verify the authenticity of the token

# HMAC

- Defined in RFC 2104 as:

H(K XOR opad, H(K XOR ipad, text))

Where:

H – Hash function (SHA256, etc.)

K – secret Key

Text – Input

opad/ipad – padding characters

# HS256 vs RS256

- If the hash function is based on a private key, then a public key can be used to verify the origin of the claim
- Makes tokens transferrable and independently verifiable.

# Protecting Access

- Access Enforcement
  - Avoid indirect object references, e.g.
  - http://host/path/../some/file/you/should/not/serve
- Input/Output Sanitization
  - XSS (Cross-site Scripting Attacks)
  - SQL Injection