2024-05-18 - Handout – Cybersecurity

We will be covering the below topics on System design with Cybersecurity.

- Introduction to cybersecurity. What is ransomware, malware, Advanced Persistent Threat (APT), Honey pot. Security Operations Center, MITRE attack framework.
- Cloud security. The different deployment models - IaaS, PaaS and SaaS, Shared responsibility model. Some information on virtualization and hypervisors.
- Encoding, encryption and decryption - Base 64, symmetric and asymmetric encryption.
- Hashing algorithms - MD5, SHA1, SHA 256. What is hashing collision.
- Application security - Secure software development life cycle (SSDLC), OWASP Top 10, some common security concerns like injection, cross-site scripting, server-side request forgery.
- Single sign on (SSO), Federated Identity login that uses OAuth.
- System design reflecting upon how to securely exchange company data with third parties. Discussion of mutual TLS (m-TLS) (depending upon our time).
- Questions and answers