Overview

- Fundamentals & policies
    - The C.I.A. security goals
        - Confidentiality
            - Encryption
            - Access control
            - Authentication
            - Authorization
            - Physical security
        - Availability
            - Physical protection
            - Computation redundancies / backups
        - Integrity
            - Backups
            - **Checksums**
            - Data correcting codes
    - A.A.A security concept
        - Assurance
            - Policies
            - Permissions
            - Protections
        - Anonymity
            - Aggregation
            - Mixing
            - Proxies
            - Pseudonyms
        - Authenticity
            - Nonrepudiation
                - Digital signatures
    - Threats and attacks
        - Eavesdropping

        - **Alteration**
        - Denial-of-service
        - **Masquerading**
        - **Repudiation**
        - **Correlation and traceback**
    - Security principles (commandments)
        - Economy of mechanism
        - Fail-safe default
        - Complete mediation
        - Open design
        - Psychological acceptability
        - Work factor
        - Compromise recording
        - Separation of principles
        - Principle of Least privilege
        - Least common mechanism
    - Some security mechanisms
        - Cryptographic
        - Authentication
        - Authorization
        - The reference monitor and isolation
        - Auditing

- Cryptography (basic)
    - Crypto system
        - Asymmetric
            - Elgamal
                - Encryption of same plaintext, generates different ciphertext
            - RSA
                - Raise to large prime number
        - Symmetric

- Attacks
    - Ciphertext-only attack
        - Determine plaintext, discover key
    - Known-plaintext attack
        - Access to plaintext-ciphertext pairs
        - Determine key
    - Chosen-plaintext attack
    - Chosen-ciphertext attack
- Substitution ciphers
    - Caesar
    - Vigenère cipher
    - One-time pads
        - Block of keys length equal to length of plaintext
    - Binary one-time pad
        - XOR
- Hill cipher
    - C = Key x M
    - M = Key inverse x C
- Transposition ciphers
    - Message shuffled around according to permutation
    - $C = \pi(M)$
    - $M = \pi^{-1}(C)$
- AES
    - 128-bit blocks
    - 128, 192, or 256-bit key
    - Sub bytes
    - Shift rows
    - Mix columns
    - Add round key
    - Modes:
        - Electronic codebook (ECB) mode
            - Patterns

        - Cipher-block chaining (CBC) mode
            - XOR before encryption
        - Cipher feedback mode (CFB)
            - C_i gets C_{i-1} after XOR
        - Output feedback mode (OFB)
            - Gets output from i-1
            - C_i gets C_{i-1} before XOR
        - Counter mode (CTR)
            - Random seed
            - Decryption similar to OFB
    - Initialization vector (IV)

- Shared key authentication
- Reflection attack
- The Diffie-Hellmann protocol key agreement

- Authentication (machines, humans)
    - Passwords
        - Dictionary attack
        - Secure passwords
        - Salt / Pepper

- Access control (DAC + MAC)
    - Access control models
        - Access control matrices
        - Access control lists ACL
        - Capabilities
        - Role-based access control RBAC
            - Role hierarchy
    - Discretionary access control
    - Mandatory access control

- Authorization
    - **OpenID & OAuth 2.0**

- Signatures, hashes, certificates
    - Cryptographic hash functions
        - Collision resistant
        - One way
        - Same length output
        - Birthday attack
        - Message authentication code (MAC)
    - Digital signatures
        - Alice encrypts with private key, Bob decrypts with Alice's public key
            - Can be done by hashing document
        - Elgamal
            - randomization
    - Digital certificates
        - **X.509 certificates –> Sign messages with the private key, use the X.509 as data**
    - **PKIs**

- Web security
    - HTTP protocol
    - HTTPS (hypertext transfer protocol over secure socket layer)
        - TLS (transport layer security) newer implementation of SSL
            - Certificate CA
            - TLS handshake
    - Cookies
        - Third party cookies
    - Sessions

- Malware, threats, and vulnerability

- Insider attacks
    - Backdoors
    - Logic bombs
- Computer viruses
- Malware attacks
    - Computer worms
    - Trojan horses
    - Rootkits
    - Zero-day attacks
    - Botnets
- Privacy-invasive software
    - Adware
    - Spyware
- Network attacks
    - IP spoofing
        - Alter source IP address
    - ARP spoofing
        - Cache poisoning
    - TCP session hijacking
        - Sequence number prediction
        - Blind injection
        - ACK storms
    - Optimistic TCP ack attack
        - Congestion-control
    - ICMP attacks (DoS attack)
        - The ping flood attack
        - Smurf attack
    - DDoS
        - Botnet
    - Cross-site scripting (XSS)
        - Persistent

        - Nonpersistent
    - Databases and SQL injection attacks
    - Packet sniffing
    - Phishing
        - Dummy web site
        - URL obfuscation
    - Eavesdropping
- Vulnerability
    - Social engineering
        - Something for something (Quid Pro Quo)
    - Programming errors

- Isolation
    - Sandbox

- Audit, accountability, intrusion
    - “surveillance”
    - Intrusion detection system IDS