Cybersecurity (COSC 3371)

2022 Spring

List of Midterm Topics

- Introduction to security *(Lecture 1)*
  - concepts and objectives (confidentiality, data integrity, system integrity, availability, non-repudiation, authenticity, privacy), important challenges (weakest link principle, process instead of product, cost and perceived value of security)
  - attacker modeling principles (safe assumptions, attacker capabilities and knowledge), rejection of security by obscurity *(Lecture 2)*
- Introduction to cryptography *(Lecture 2)*
  - general model of symmetric-key ciphers (plaintext, secret key, encryption, ciphertext, decryption)
  - basic types of attacks (brute force vs. cryptanalysis, ciphertext only vs. known plaintext attack)
  - Kerckhoffs's principle *(Lecture 3)*
- Stream ciphers *(Lecture 3)*
  - perfect security and one-time pad (idea, requirements, and properties)
  - basic notion of semantic security (advantage of efficiently computable attack over random guessing), problem with "many-time pad"
  - general model of stream ciphers
  - pseudorandom number generators (key requirements, including resistance to cryptanalytic and brute-force attacks)
  - key-reuse problem and solutions
  - RC4 and Salsa20 (basic properties) *(Lecture 4)*
- Block ciphers *(Lecture 4)*
  - general model of block ciphers
  - design considerations and security
  - practical design principles (diffusion and confusion)
  - idea and structure of iterated block ciphers
  - idea and structure of substitution-permutation ciphers
  - DES
    - very basic properties (e.g., state of security, approximate block and key sizes)
    - Feistel-network: structure and advantages
  - AES
    - basic properties (e.g., state of security, performance, block and key sizes)
    - high-level structure and general properties (e.g., invertibility) of the substitution and permutation steps (SubBytes, ShiftRows, MixColumns)
  - 3DES *(Lecture 5)*
    - principle of multiple encryption, meet-in-the-middle attack
    - motivation for 3DES and EDE structure

- Block cipher modes of operation *(Lecture 5)*
  - ECB, CBC, OFB, and CTR modes of operation
  - structure and properties of each mode, including security (information leakage, tampering), performance (parallelization, seeking), and error propagation
- Public-key encryption *(Lecture 6)*
  - principles of public-key cryptography (asymmetric pair of keys)
  - general model and requirements for public-key encryption schemes, comparison with symmetric-key cryptography
  - RSA
    - key ideas for algorithms and security, hardness of integer factorization, security and efficiency (approximate key sizes)
  - ElGamal
    - hardness of discrete logarithm
  - Elliptic Curve Cryptography
    - basic idea (replacing modular arithmetic with elliptic curves) and advantages
- Hash functions *(Lecture 7)*
  - general model and applications
  - formal requirements (one way, weak collision resistant, strong collision resistant)
  - brute-force attacks and birthday paradox
  - structure of iterative hash functions, Merkle-Damgård construction
  - basic properties and state of security for MD5, SHA-1, SHA-2, and SHA-3
- Message authentication *(Lecture 8)*
  - active attacks in a communication channel *(Lecture 7)*
  - general model of message authentication, usage and properties of MAC tags
  - brute-force tag forging and key search attacks
  - MAC based on block ciphers (structure of CBC-MAC, basic idea of CMAC)
  - MAC based on hash functions (structure of HMAC, advantages in terms of precomputation and security)
  - authenticated encryption
    - motivation and approaches
    - very basic properties of CCM and GCM
- Digital signatures *(Lecture 9)*
  - motivation (non-repudiation requirement), general model, usage, and properties of digital signatures
  - relation to public-key encryption
  - hash-then-sign principle
  - very basic properties of RSA signature, DSA, and ECDSA
- Key distribution *(Lectures 9)*
  - requirement of key freshness, idea of key hierarchy (session and master keys)
  - symmetric-key distribution using symmetric encryption
    - decentralized: advantages and disadvantages
    - Key Distribution Center: advantages and disadvantages
  - ideas of extended Needham-Schroeder and Kerberos protocols

- Public-key distribution *(Lecture 10)*
  - symmetric-key distribution using asymmetric-key cryptography
    - Diffie-Hellman key exchange, idea of Station-to-Station
    - idea of symmetric-key distribution using asymmetric encryption
  - distribution of public keys
    - motivation, problems with basic approaches (public announcement and public-key authority)
  - digital certificates
    - process (requesting/issuing and using), requirements, advantages
    - usage of X.509 standard, certificate authorities in practice
    - problem with private key compromise, process of revocation