Midterm Review (I): Crypto

Dawn Song
dawnsong@cs.berkeley.edu

Formal/Advanced Crypto

- **This class is a quick intro**
- **Interested in further study**
  - **Crypto class**
    - » **Formal definitions & proofs**
    - » **Advanced algorithms & protocols**
- **Class & midterm will be self-contained**

Basic Background

- **Probability calculation as seen in hw**
  - **E.g., Birthday paradox**
- **Basic algebric calculation as seen in hw**

Attacker's Mindset

- **A lot of security training is about "attacker mindset"**
  - **Given a design (e.g., protocol), find attacks**
- **Important for designing secure systems**

Security Design & Evaluation

- **Security goals**
  - **CIA: confidentiality, integrity, availability**
- **Threat model**
  - **Assumptions about attacker**
- **Security analysis**

Symmetric-key Encryption

- **What security goal does it achieve?**
  - **Confidentiality**
- **Threat model**
  - **Known ciphertext attack**
  - **Known plaintext attack**
  - **Chosen plaintext attack (CPA)**
  - **Chosen ciphertext attack (CCA)**
- **One-time pad**
  - **How does it work?**
  - **What security property does it achieve?**
    - » **Attacker without computation limitation**
  - **Requirement for security**
    - » **Key is same length as message**
    - » **Cannot reuse key**

Ciphers

- **Stream cipher**
  - **How does it work?**
  - **What's the difference btw stream cipher & one-time pad?**
    - » **Stream cipher is secure assuming attacker is polynomial time bounded**
- **Block cipher**
  - **Modes of operation**
    - » **How does each mode work?**
    - » **Disadvantage of ECB**
      - **Same plaintext always encrypt to same ciphertext**
    - » **Security requirements for CBC, OFB, CTR**
      - **Cannot reuse IV**

Asymmetric-key Crypto

- **Advantages over symmetric-key crypto**
- **Disadvntages over symmetric-key crypto**
  - **Performance overhead**
- **Additional requirements**
  - **PKI**
- **RSA**
  - **How does it work?**
  - **Why is textbook RSA not a secure encryption scheme?**
    - » **Deterministic, short-plaintext attack**

Hash Function

- **Security properties**
  - **Preimage resistance**
  - **2nd-preimage resistance**
  - **Collision resistance**
  - **What do they mean and when to use which one?**

Message Authentication Code (MAC)

- **Security property**
  - **Unforgeability**
    - » **What does it mean?**
- **What security goal does it achieve?**
  - **Integrity**

Digital Signature

- **Security property**
  - **Unforgeability**
- **What security goal does it achieve?**
  - **Data integrity & non-repudiation**
- **How to compare MAC with Digital Signature?**
- **Additional requirements**
  - **PKI**
- **RSA signature scheme**

Authentication & Key Distribution

- **Attacks on security protocols**
  - **Active attacker model**
  - **Should be able to spot simple attacks like in Needham-Schroeder**
- **Diffie-Hellman key agreement**
  - **What's man-in-the-middle attack?**
- **Password authentication protocol**
  - **What's a dictionary attack?**
  - **Given a protocol, should be able to tell if it is vulnerable to dictionary attack**
- **Do not need to know how each protocol works in detail**

Random Number Generation

- **Two steps**
  - **TRNG (true random number generator)**
    - **What sources are good and what sources are bad?**
  - **PRNG (cryptographically secure pseudorandom number generator)**
- **Important for many security applications**
  - **Generating IV, keys, etc.**

Secret Sharing

- **Definition of (n,n) and (n,t) threshold scheme**
- **How do they work?**
- **Should be able to solve problems like in hw**
- **Zero-knowledge proof**
  - **Out of scope**