6.1600 Midterm 1 Review Session

October 2024

1 Encryption Security Concepts

1.1 CPA Security

- Adversary gets 1^n where n is the length of the key
- For $poly(n)$ rounds, adversary gets access to the function $m \leftrightarrow E_k(m)$
- Adversary chooses pair of messages $\{m_0, m_1\}$, a secret b is chosen at random from $\{0, 1\}$, and adversary gets $c^* = E_k(m_b)$
- Adversary now gets another $poly(n)$ rounds of access to the functions $m \leftrightarrow E_k(m)$
- Adversary outputs b' and wins if $b' = b$

Intuitively: Adversary cannot find out information about the plaintext even when given access access to encryption process.

1.2 CCA Security

An encryption scheem (E, D) is CCA secure if every efficient adversary wins the followign game with probability at most $\frac{1}{2}$ + negligible.

- Adversary gets 1^n where n is the length of the key
- For $poly(n)$ rounds, adversary gets access to the function $m \leftrightarrow E_k(m)$ and $c \leftrightarrow D_k(c)$
- Adversary chooses pair of messages $\{m_0, m_1\}$, a secret b is chosen at random from $\{0, 1\}$, and adversary gets $c^* = E_k(m_b)$
- Adversary now gets another $poly(n)$ rounds of access to the functions $m \leftrightarrow E_k(m)$ and $c \leftrightarrow D_k(c)$ except that she is not allowed to query c^* to her second oracle.
- Adversary outputs b' and wins if $b' = b$

Intuitively: Adversary cannot find out information about plaintext even when given access to encryption and decryption process.

1.3 Encryption with Authentication

Encrypt then MAC is CCA secure. However, a few notes:

- Cannot use same key for encryption and MAC
- MAC then Encrypt is not CCA secure
- Need to MAC the entire ciphertext
- Cannot output some plaintext before verifying integrity

Intuitively: Encrypt then MAC gives us CCA security because we don't want our ciphertext to be tampered with. Hence, we need to ensure authentication.

1.4 Diffie-Hellman Protocol

Example of quick step through of the Diffie-Hellman protocol:

- Alice and Bob publicly agree to use modulus $p = 23$ and $g = 5$
- Alice chooses a secret integer $a = 4$, then sends Bob $A = g^a \bmod p = 4$
- Bob chooses a secret integer $b = 3$, then sends Alice $B = g^b \bmod \text{p} = 10$
- Alice computes $s = B^a \bmod p = A^b \bmod p = 18$, which becomes their shared secret.

1.5 Computational Diffie-Hellman Assumption

Given (g, g^a, g^b) for randomly chosen $a, b \in \{0, \dots, q-1\}$, it is computationaly intractable to compute the value g^{ab}.

2 Terms you've Probably Heard

- Hash
- MAC
- Digital Signature
- AES
- PRF
- Symmetric Key
- Diffie-Hellman
- RSA
- CRHF
- Elliptic Curve Cryptography
- Collision Resistance
- PKI
- TLS

3 Problems with Encryption

- Cannot hide message lengths
  - Padding
- Source is still known
  - TOR
- Compromised server
  - Private Information Retrieval