2.1 Basic Cryptography Concepts

Min Wu

Electrical and Computer Engineering
University of Maryland, College Park

http://umd.blackboard.com (select ENEE739B); minwu@eng.umd.edu
Part of the slides are used or revised from material courtesy of Prof. Y. Sun of Univ. Rhode Island.

Outline: Basic Security/Crypto Concepts

- Typical scenarios and attacks on secure communications
- Kerckhoff principle
- Major security aspects
- Symmetric vs. Asymmetric encryption

Crypto Terminologies

- Cryptography: the art of secret writing
  - The art of mangling information into apparent unintelligibility in a manner that allows a secret method of unmanaging.

- Three related terminologies
  - Cryptology: The study of communication over non-secure channels, and related problems
  - Cryptography: The process of designing systems that achieve secure communications.
  - Cryptanalysis: Breaking such systems. (The techniques used to recover the secret information hidden in cryptographic systems)

They are often used interchangeably.

Basic Secure Communication Scenario

- Plaintext: the message in its original form
- Ciphertext: the mangled information
- Encryption: the process of produce ciphertext from plaintext
- Decryption: the process reversing the encryption

Encryption and Decryption involve some Algorithm and secret values (keys)
### Adversaries

**Eve’s Goal**
1. Read the message
2. Figure out the key Alice is using and read all the messages encrypted with that key
3. Modify the content of the message in such a way that Bob will think Alice sent the altered message.
4. Impersonate Alice and communicate with Bob who thinks he is communicating with Alice.

**Passive observer “Olive”**

**Active adversary “Mallory”**

### Attack Methods

- **Ciphertext only**
  - Eve has only a copy of ciphertext

- **Known Plaintext**
  - Eve has ciphertext and the corresponding plaintext, and tries to deduce the key.

- **Chosen Plaintext** *
  - Eve has ciphertext corresponding to some plaintext selected by her, believing it useful to deduce the key.

- **Chosen Ciphertext** *
  - Eve has a copy of plaintext corresponding to a copy of ciphertext selected by her, believing it is useful to deduce the key.

* Possible when Eve gains temporary access to encrypter / decrypter

### Kerckhoff’s Principle

- Relying on secrecy of the crypto algorithm?
  - Hard to quantify the security strength
    - *some thinking process of people may be alike*
    - *may have to abandon the entire system when compromised*

  => Should always assume an adversary knows the crypto algorithm used when assessing a cryptosystem’s strength

- The security of a crypto system should be based on
  - the quality/strength of the algorithm but not its obscurity
  - secrecy of the key over a sufficiently large key space (or key length)

### Major Cryptographic Objectives

- **Confidentiality**
  - Hide the contents of a message from unauthorized observer
  - Main tools: encryption / decryption

- **Data integrity**
  - Ensuring the message sent has not been altered
  - Main tools: hash functions to detect tampering

- **Authentication: entity identification & data-origin authentication**
  - Correctly verify a user’s identity: through password protocol
  - Verify the origin of a message (creator, creation time, etc)

- **Non-repudiation**
  - A sender cannot deny a transmitted message or transaction
**Data Confidentiality**
- Eve should not be able to read Alice’s message to Bob.
- The oldest and best known aspect of data security.
  - The main tools are encryption / decryption

**Data Integrity**
- Bob wants to be sure that Alice’s message has not been altered.
  - Transmission errors may occur
  - An adversary might intercept the transmission and alter it.

**User Authentication**
- Password protocol
  - When you log on to a computer, the computer need to identify your identity.
- Verify communication partner
  - Verify that we are communicating with the right person.

**Data Origin Authentication**
- Authenticate the information about the origin of the data, such as the creator and time of creation.
  - Bob wants to make sure that the message is really from Alice, and the message was not a replay of previous messages from Alice.
Non-repudiation

- Alice cannot claim that she did not send the message.
  - Suppose Bob takes orders from his customer through emails. Alice made an order through email and later denied this purchase. Bob needs to show that Alice did send the email.

- Data-origin authentication vs. non-repudiation
  - In a paper and pencil world, non-repudiation is provided by a manual signature.
  - Hard to show non-repudiation in symmetric-key crypto.
  - Public-key crypto can do both.

Symmetric Key Cryptography

- Alice and Bob know both the encryption key and the decryption key.
  - Encryption key and decryption keys are the same.
  - The encryption key is shared and the decryption key is easy to be calculated from the encryption key.

- Symmetric cryptosystems:
  - All of the classical (pre-1970) systems
  - DES and AES

  **Challenge:** Alice and Bob need to agree upon a key.

Public Key Cryptography

- What if Alice and Bob cannot hold a common key?
  - A nonmathematical way
    - Bob: send Alice a box and an unlocked padlock.
    - Alice: put her message in the box, lock it using Bob’s lock, and send the box back to Bob.
    - Bob can open the box and read the message.

- Public key cryptography (asymmetric cryptography)
  - The encryption key is made public.
  - The decryption key is only known by Bob.
  - It is computationally infeasible to find the decryption key without information known only to Bob.
**Symmetric versus Asymmetric Encryption**

- Public key cryptography is several orders of magnitude more expensive than symmetric one
  - On a Pentium PC, \( DES: 15 \text{ Mbit/s encryption rate} \)
  - \( AES: 6 \text{ Kbits/s encryption rate} \)
  - DES is typically 1000 times faster than the RSA-scheme

- Public-key systems provide significant benefits in terms of key management:
  - Assume \( n \) users want to securely communicate to each other.
    - Symmetric: \( n(n-1)/2 \) keys
    - Asymmetric: \( 2n \) keys

- Hybrid system
  - Using a public-key system for distributing secret “session key”
  - A symmetric cipher for the bulk encryption of the data

---

**Key Length**

- Brute force attack: try every possible key and see which one yields meaning decryption.
  - \( DES: 2^{56} \approx 7.2 \times 10^{16} \) possibilities

- Longer keys are advantageous, but not guaranteed to make an adversary’s task difficult.
  - Not all 128-bit algorithms are equally secure
  - Guessing the keys is often only one of many ways to break/attack the system.
  - Public-key crypto usually requires longer keys
    - owing to the cipher structure that allows for asymmetry

---

**Key Length (cont’d)**

- Key sizes for symmetric ciphers
  - 40 bits (\( 2^{40} \approx 10^{12} \)) were used in the 1980s and 1990s in Internet applications
  - 56 bits (\( 2^{56} \approx 10^{17} \)) are used by DES, good in the 1980s; not strong enough today.
  - 64 bits (\( 2^{64} \approx 10^{20} \)) are used by some ciphers today.
  - 128 bits (\( 2^{128} \approx 10^{40} \)) are considered the smallest number of bits to be used by modern algorithms today.

- An algorithm secure today does not mean an algorithm secure in the future

---

**Summary**

- Typical scenarios and attacks on secure communications
  - Understand attacker’s goals and strategies

- Kerckhoff principle:
  - Should assume algorithm is known but key unknown
  - Rely on algorithm’s strength and key space

- Major security aspects: C.I.A.N.
  - Confidentiality, Integrity, Authentication, Non-repudiation

- Symmetric vs. Asymmetric encryption

- Next time:
  - Encryption basics
**Preview of Next Sections: Basic Crypto Tools**

- **Symmetric Encryption**
  - Substitution cipher
  - Block cipher: DES, AES
  - Stream cipher: one-time pad
- **Random number generators**
- **Asymmetric Tools**
  - Based on discrete math / algebra
  - Encryption: RSA
  - Key establishment: Diffie-Hellman
- **One-way functions**
  - Hash / Message Digest

^ to be covered in Section 2.2

---

**Reading Assignment**

- **HAC (Handbook on Applied Crypto) Chapt. 1 Overview**
  
  http://www.cacr.math.uwaterloo.ca/hac/

  Students new to crypto background may find the online survey on crypto concepts “Cryptography A-Z” a helpful start
  
  http://www.ssh.fi/support/cryptography/

  and/or Trappe-Washington’s Crypto textbook Chapt. 1

- **Bruce Schneier, “Why Cryptography Is Harder Than It Looks.”**
  
  http://www.schneier.com/essay-whycrypto.html