Lecture 24: A Review of Major Cryptographic Primitives

Cunsheng DING, HKUST

COMP3631

The objective of this review lecture

The objective of this lecture is to recall the answers to the following questions:

1. What are the security services covered in this course?
2. How is the data confidentiality service provided?
3. How are the data origin authentication and data integrity services provided simultaneously?
4. How is the mutual authentication service provided?
5. How is the anti-replay service provided?
6. How is a common secret key established?

Passive and active attacks

Question: What are passive and active attacks?

Question: What is the replay attack?

Question: Is the replay attack a passive attack?

Question: Could the replay attack be a serious security problem?

Question: How is the anti-replay service provided?

Attentions: If a security system is secure with respect to active attacks, it must be secure with respect to passive attacks by definition.

However, even if a security system is secure with respect to passive attacks, it may not be secure with respect to active attacks (e.g., the DH protocol).

A summary of the security services covered

- Data confidentiality
- Data origin authentication, sender authentication, receiver authentication, mutual authentication
- Data integrity (data authentication)
- Signer nonrepudiation
- Anti-replay
- Anonymity
- Key generation, key distribution, key establishment

Comment: You should fully understand these security services and know how these security services are provided.

The data confidentiality service

A one-key stream cipher is normally used to encrypt a piece of data m. The ciphertext $E_k(m)$ may be in storage or in transmission in the form:

$$\text{Alice } \rightarrow E_k(m)||ID_A||ID_B \rightarrow \text{ Bob}$$

Encryption is usually done with a one-key block cipher in the CBC mode.

Question: Does this protocol provide other security services? If yes, what are these security services?

Answer: It depends on if m contains a timestamp, ID of sender/receiver or if m has **"redundancy"**.

Attention: Whatever cipher (e.g., the One-Time-Pad) is used, an attacker may guess the secret key correctly and may be able to decrypt the ciphertext. But this probability is very small if the cipher is well designed.

The redundancy of messages

Redundancy: The unnecessary part in a message. E.g., the redundancy in "tomorrow" is at least one letter without loosing its meaning, as it can be compressed into "omorrow" or "tmorrow" or "toorrow" or "tomrrow" or "tomorow" or "tomorrw" or "tomorro".

Measure of redundancy: A rigorous measure of redundancy can be given with the Shannon information theory. This is out of the scope of this course.

Some remarks on redundancy:

- Every human language has redundancy. This is for error detection and error correction. English has more redundancy than Chinese.
- Data redundancy makes data-compression-and-decompression possible.

Data origin authentication & data integrity (1)

Question: How are the two security services **simultaneously** provided?

Answer: In real-world security systems, two protocols are used.

Data origin authentication & data integrity (2)

In PGP and S/MIME, the two security services are provided in the form:

$$\text{Alice} \rightarrow m||\text{Alice's digital signature on } m||ID_A||ID_B \rightarrow \text{Bob}.$$

Attention: If the digital signature scheme is well designed, signature forgery and data modification can be detected with high probability. Hence, it provides the singer nnonrepudiation service.

Question: What should Bob do after receiving the text from Alice?

Question: Does this protocol provide other security services (e.g., when m contains a timestamp)?

Data origin authentication & data integrity (3)

In most real-world security systems, the two security services are provided simultaneously as follows:

$$\text{Alice } \rightarrow m||h_k(m)||ID_A||ID_B \rightarrow \text{Bob},$$

where a hash function h and an authentication key are used in the HMAC mode for obtaining a keyed hash function h_k. The HMAC approach was covered earlier.

The value $h_k(m)$ is called the **message authentication code** (MAC).

Question: What should Bob do after receiving the text from Alice?

Question: Does this protocol provide other security services such as the antireplay?

Providing the mutual authentication (1)

Question: How is the mutual authentication service provided?

Answer: In real-world security systems, three protocols are used.

Providing the mutual authentication (2)

The following authentication protocol (used also in the Kerberos protocol):

$$\text{Alice } \rightarrow E_k(Timestamp_1||ID_A||ID_B)||ID_A||ID_B \rightarrow \text{ Bob},$$

$$\text{Alice } \leftarrow ID_A||ID_B||E_k(ID_A||ID_B||Timestamp_2) \leftarrow \text{ Bob},$$

where a pre-shared secret key k of the one-key cipher and timestamp are used.

Question: Does this protocol provide other security services such as the data integrity and antireplay?

Question: What are the two purposes of adding the timestamp in this protocol? (hint: anti-? and sender ??)

Providing the mutual authentication (3)

The following challenge-response protocol:

$$\text{Alice } \rightarrow E_{k_e^{(B)}}(N_1)||ID_A||ID_B \rightarrow \text{ Bob},$$

$$\text{Alice } \leftarrow ID_A||ID_B||E_{k_e^{(A)}}(N_1||N_2) \leftarrow \text{ Bob},$$

$$\text{Alice } \rightarrow E_{k_e^{(B)}}(N_2)||ID_A||ID_B \rightarrow \text{ Bob},$$

where N_i are nonces, ID_A and ID_B are the ID of Alice and Bob, respectively. They know the ID of each other.

Question: Does this protocol provide other security services such as the data integrity?

Providing the mutual authentication (4)

The following authentication protocol (using the digital signature):

$$\text{Alice} \rightarrow D_{k_d^A}(timestamp_1||ID_A||ID_B)||ID_A||ID_B \rightarrow \text{Bob}$$
$$\text{Alice} \leftarrow ID_A||ID_B||D_{k_d^B}(ID_A||ID_B||tiemstamp_2) \leftarrow \text{Bob}$$

Alice and Bob have exchanged their public keys and IDs.

Question: Why could this protocol provide the mutual authentication service?

Question: Does this protocol provide other security services such as the data integrity and antireplay?

Providing the signer nonrepudiation service

Protocols: In real-world security systems, the following two digital signature schemes are supported:

- The RSA public-key cipher and a hash function.
- The Digital Signature Standard (also called DSA).

Establishing a common secret key (1)

Recall: We talked about key generation, key distribution, key exchange.

Remark: Key management includes, key generation, key distribution, key exchange, key storage, key destruction, etc.

Comment: Key management is the most complicated building block in real-world security systems!

Information: Two protocols for establishing a common secret key are supported in real-world security systems.

Establishing a common secret key (2)

The first one is the digital-envelop (DE) protocol,

$$\text{Alice } \rightarrow E_{k_e^B}(k)||ID_A||ID_B \rightarrow \text{Bob},$$

where we assume that all public keys and IDs are in the public domain.

Question: Is this protocol secure with respect to man-in-the-middle attacks.

Answer: No. Eva can replace $E_{k_e^B}(k)$ with $E_{k_e^B}(k')$ in the middle of transmission and pretends that she is Alice. In this way, Eva will be able to establish a secret key k' with Bob and pretends that she is Alice.

Question: Why is it used in real-world security systems?

Embedding the DE into a mutual authentication protocol

The merged protocol:

$$\text{Alice } \rightarrow E_{k_e^{(B)}}(N_1)||ID_A||ID_B \rightarrow \text{ Bob},$$

$$\text{Alice } \leftarrow ID_A||ID_B||E_{k_e^{(A)}}(N_1||N_2) \leftarrow \text{ Bob},$$

$$\text{Alice } \rightarrow E_{k_e^{(B)}}(k||N_2)||ID_A||ID_B \rightarrow \text{ Bob},$$

where k is a session key generated by Alice, N_i are nonces, ID_A and ID_B are the ID of Alice and Bob, respectively. They know the ID of each other.

Establishing a common secret key (3)

The second one is the Diffie-Hellman key exchange protocol. Let us recall this protocol briefly (see Lecture 14).

Question: Is this protocol secure with respect to man-in-the-middle attacks.

Question: Why is it used in real-world security systems?

Diffie-Hellman group: a specific pair (p, α) used in the Diffie-Hellman protocol.

Embedding the DH into a mutual authentication protocol

The following merged protocol:

$$\text{Alice } \rightarrow E_{k_e^{(B)}}(Y_A||N_1)||ID_A||ID_B \rightarrow \text{ Bob},$$

$$\text{Alice } \leftarrow ID_A||ID_B||E_{k_e^{(A)}}(N_1||N_2||Y_B) \leftarrow \text{ Bob},$$

$$\text{Alice } \rightarrow E_{k_e^{(B)}}(N_2)||ID_A||ID_B \rightarrow \text{ Bob},$$

where Y_A and Y_B are the DH values of Alice and Bob, N_i are nonces, ID_A and ID_B are the ID of Alice and Bob, respectively. They know the ID of each other.

Applications of the cryptographic primitives

The cryptographic primitives covered in this course are used in real-world security systems such as

- Operating systems (for password protection and intrusion detection);
- PGP and S/MIME (for protecting email communication);
- IP Security (for networking security);
- SSL/TLS (for Web security);
- VPNs (for establishing a secure channel between two computers); and
- Secure Shell (for establishing a secure channel between two computers).

These important applications show that cryptography is the foundation of computer security and cybersecurity.