Security Solutions in Security Systems

Cunsheng DING, HKUST

April 21, 2022

Security Solutions in Security Systems

Outline of this document

1. How to provide the data confidentiality service?
2. How to provide the sender authentication and data integrity?
3. How to provide the mutual authentication service?
4. How to establish a common secret key?

Information about this document

The first part (i.e., cryptography) of this course covers security mechanisms for providing specific security services. Some of them will be used in real-world security systems such as PGP and S/MIME, IP Security, Kerberos, SSL/TLS, VPNs and the Secure Shell, which are covered in the second part of this course. To save time and understand these real-world security systems, you must read this document at the **appropriate time**.

COMP4631 students should read this document right after Lecture 14 but before Lecture 15. COMP5631 and CSIT5710 students should read this document right after Lecture 14 but before Lecture 16.

Providing the confidentiality service

A cipher is used to encrypt a piece of data m. The ciphertext $E_k(m)$ may be in storage or in transmission:

$$\text{Alice } \rightarrow E_k(m) \rightarrow B$$

Encryption is usually done in CBC mode.

Providing sender authentication and data integrity

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

$$\text{Alice } \rightarrow m||\text{Alice' digital signature on } m \rightarrow B.$$

In most real-world security systems, the two security services are provided in the form:

$$\text{Alice } \rightarrow m||h_k(m) \rightarrow B,$$

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.

Providing mutual authentication

Type-1 authentication protocol using a pre-shared secret key k (a Kerberos-like protocol or Niederheim-Schroeder-like protocol),

$$\text{Alice } \rightarrow E_k(ID_A||ID_B||timestamp) \rightarrow B$$
$$\text{Alice } \leftarrow E_k(ID_B||ID_A||timestamp) \leftarrow B$$

Type-2 authentication protocol (a challenge-response protocol),

$$\text{Alice } \rightarrow E_{k_e^B}(N_1) \rightarrow B$$
$$\text{Alice } \leftarrow N_1 \leftarrow B$$

This is to allow Alice to authenticate Bob. Authentication in the other direction is similar.

Type-2 authentication protocol with the digital signatures of the parties.

Establishing a common secret key

The first one is the digital-envelop method,

$$\text{Alice } \rightarrow E_{k_e^B}(k) \rightarrow B$$

The second one is the Diffie-Hellman protocol.

Both are used after the mutual authentication. Hence, they are secure with respect to man-in-the-middle attacks.

If both protocols are supported in a security system, the two communicating parties must negotiate one of them.