Computer Systems Security

Dr. Ayman Abdel-Hamid

College of Computing and Information Technology

Arab Academy for Science & Technology and
Maritime Transport

Key Distribution in Symmetric Encryption

Outline

- Key Distribution in Symmetric Encryption
  - Key distribution alternatives
  - The role of a KDC and a hierarchy of keys
  - A key distribution scenario
  - Key distribution issues

Key Distribution in Symmetric Encryption 1/6

- symmetric schemes require both parties to share a common secret key
- issue is how to securely distribute this key
- often secure system failure due to a break in the key distribution scheme

Key Distribution in Symmetric Encryption 2/6

- given parties A and B → various **key distribution** alternatives:
  1. A can select key and physically deliver to B
  2. third party can select & deliver key to A & B
  3. if A & B have communicated previously can use previous key to encrypt a new key
  4. if A & B have secure communications with a third party C, C can relay key between A & B

Key Distribution in Symmetric Encryption 3/6

- given parties A and B → various **key distribution** alternatives:
  1. A can select key and physically deliver to B
  2. third party can select & deliver key to A & B
     - Manual delivery of a key
     - awkward for end-to-end encryption
     - A key is needed for each pair of communicating entities (for N entities → number of required keys is N(N-1)/2. What is an entity?)

Key Distribution in Symmetric Encryption 4/6

- given parties A and B → various **key distribution** alternatives:
  3. if A & B have communicated previously can use previous key to encrypt a new key
     - If an attacker ever succeeds in gaining access to one key, all subsequent keys will be revealed
     - Initial distribution of a large number of keys must still be made

Key Distribution in Symmetric Encryption 5/6

- given parties A and B → various **key distribution** alternatives:

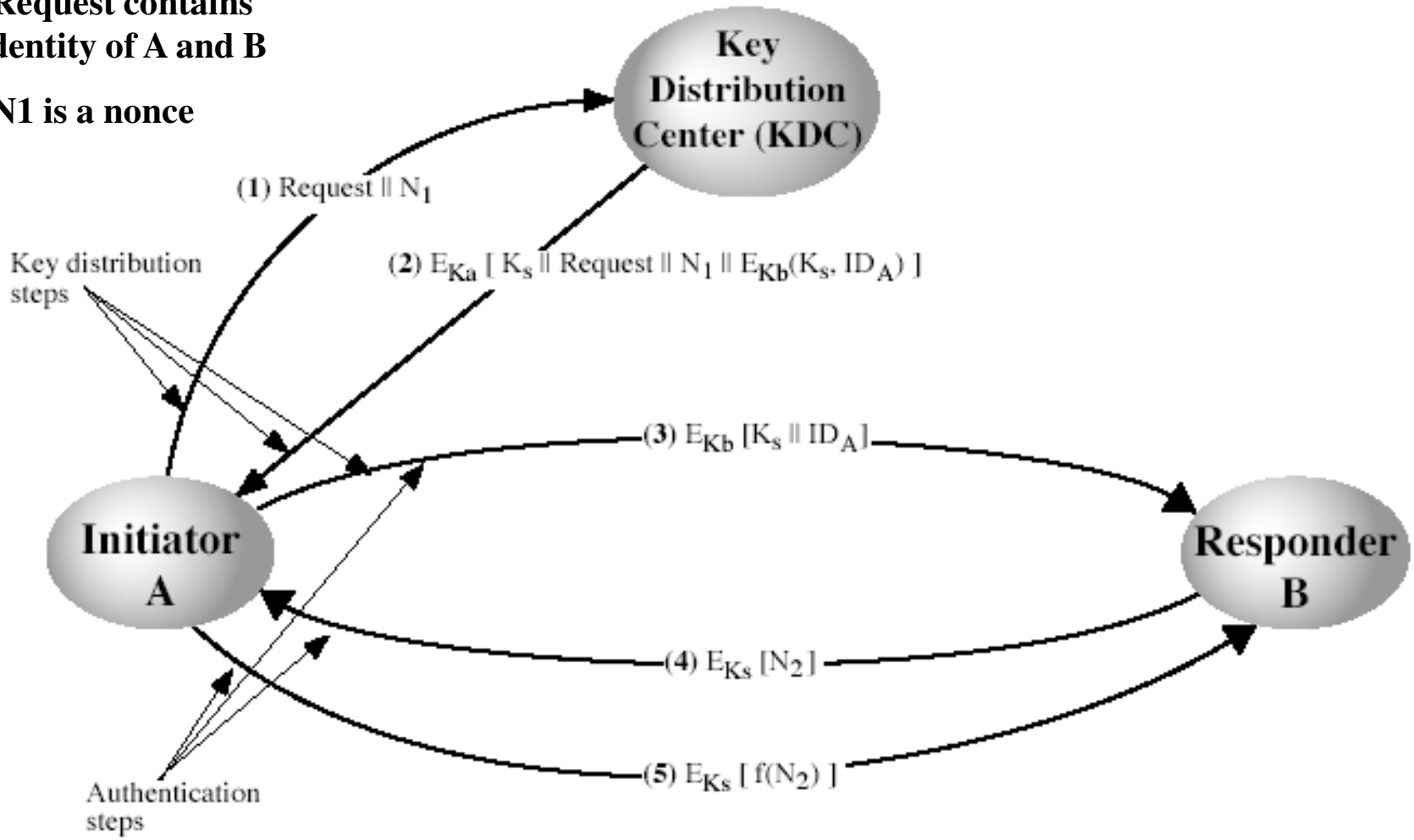
4. if A & B have secure communications with a third party C, C can relay key between A & B
   - A *key distribution center* (KDC) is responsible for distributing keys to pairs of entities (hosts, processes, or applications)
   - Each user must share a unique key with the KDC for the purposes of key distribution

Key Distribution in Symmetric Encryption 6/6

- Use of a KDC is based on use of a hierarchy of keys
  → At a minimum 2 levels of keys
- Session key
  - Temporary key used to encrypt communication between end systems
  - Used for duration of logical connection and then discarded
  - Obtained from KDC
- Master key
  - Shared by KDC and end system or user
  - Used to encrypt session keys while being transmitted from KDC to end system
  - Still need to be distributed (How many master keys are needed?)

Key Distribution Scenario

- **Request contains identity of A and B**
- **N1 is a nonce**

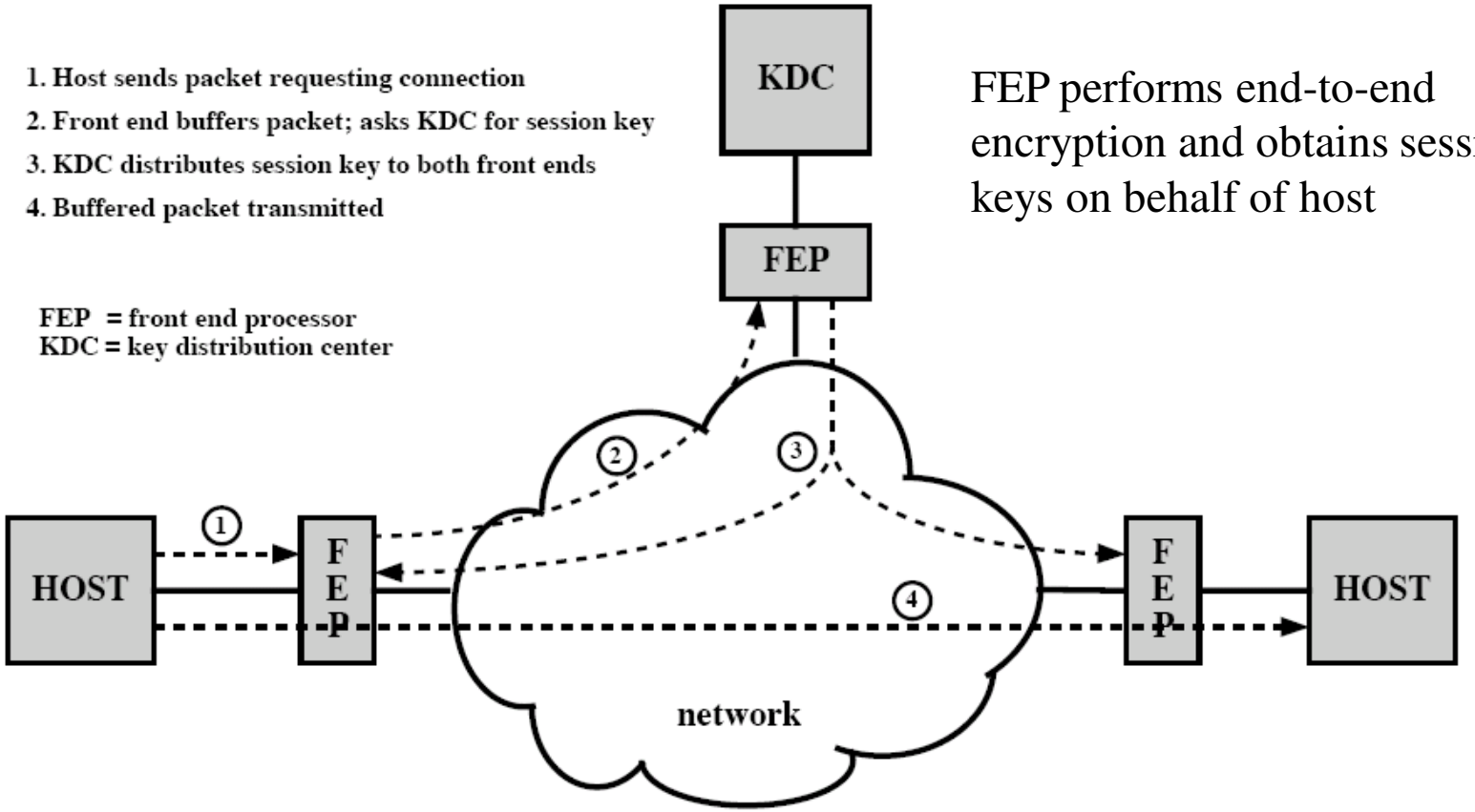


Key Distribution Issues 1/3

- Hierarchies of KDC's required for large networks, but must trust each other
  - Local KDC for communication among entities within the same domain
  - For entities in different local domains, local KDCs can communicate through a global KDC
- Session key lifetimes should be limited for greater security
  - Connection-oriented protocols (length of time connection is open → if too long?)
  - Connectionless protocols

Key Distribution Issues 2/3

•use of automatic key distribution on behalf of users (transparent to the end user), but must trust system



FEP performs end-to-end encryption and obtains session keys on behalf of host

Key Distribution Issues 3/3

•use of decentralized key distribution