

Miscellaneous Security Topics

This module is meant to cover any left over ideas which are important for the Computer and Network Security Course

Agenda

- Principal Authentication
- Intrusion Detection
- Key Management

Principal Authentication

- Three factors
- What you know?
 - ⊗ Passwords
 - ⊗ Pass phrases
 - ⊗ Answers to questions
- What you have?
 - ⊗ A smart card with your public key
- What you are?
 - ⊗ Biometrics
 - ⊗ Face recognition
 - ⊗ Finger print
 - ⊗ Retina pattern
 - ⊗ Voice recognition

Problems with Passwords

- Clear-text vs. Encrypted
- Challenge Response to prevent replay
- Dictionary attacks

Problems with Biometrics

- Developing technology
- Costs
- False Pass and False Fail are possible

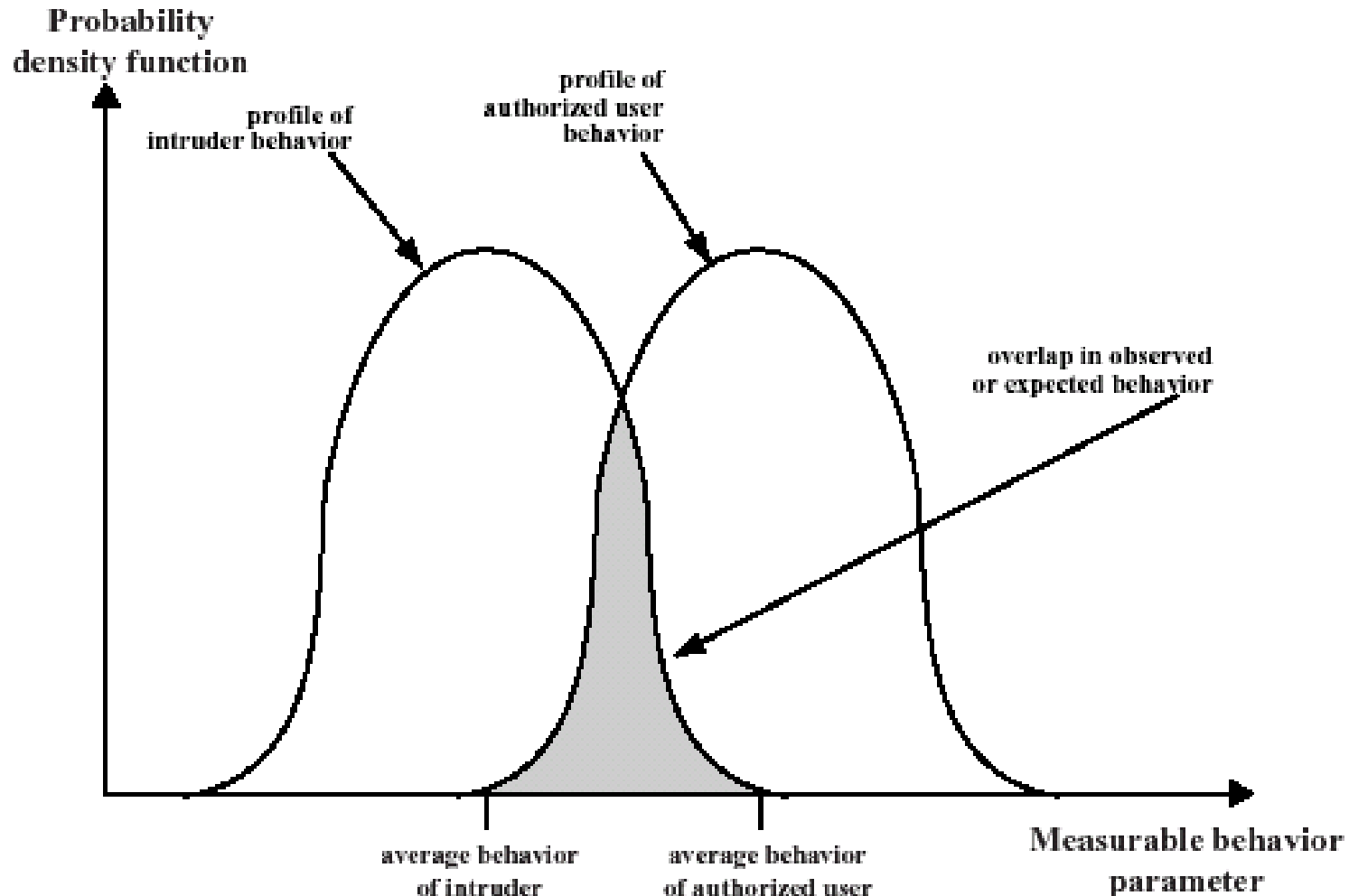
Intruders and Intrusion

- The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system
- **Masquerader** – an individual who is not authorized to use the computer and who penetrates system's access controls to exploit a legitimate user's account
- **Misfeasor** – a legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuse his.her privilege
- **Clandestine User** – an individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit information

Intrusion Detection

- Intrusion prevention tries to limit unauthorized access by using various techniques such as passwords, access control lists, etc.
- Even the best intrusion prevention systems can fail – next best thing is detection of intrusion and taking of corrective action – ejection of intruder
- This can even serve as a deterrent
- Can learn from intrusion events detected to prevent future intrusion

Profiles of Behavior of Intruders and Authorized Users



Approaches to Intrusion Detection

■ Statistical Anomaly Detection

- ⊗ Involves the collection of data relating to behavior of legitimate users over a period of time. Applies statistical tests to determine with high confidence level if the behavior is not legitimate user behavior

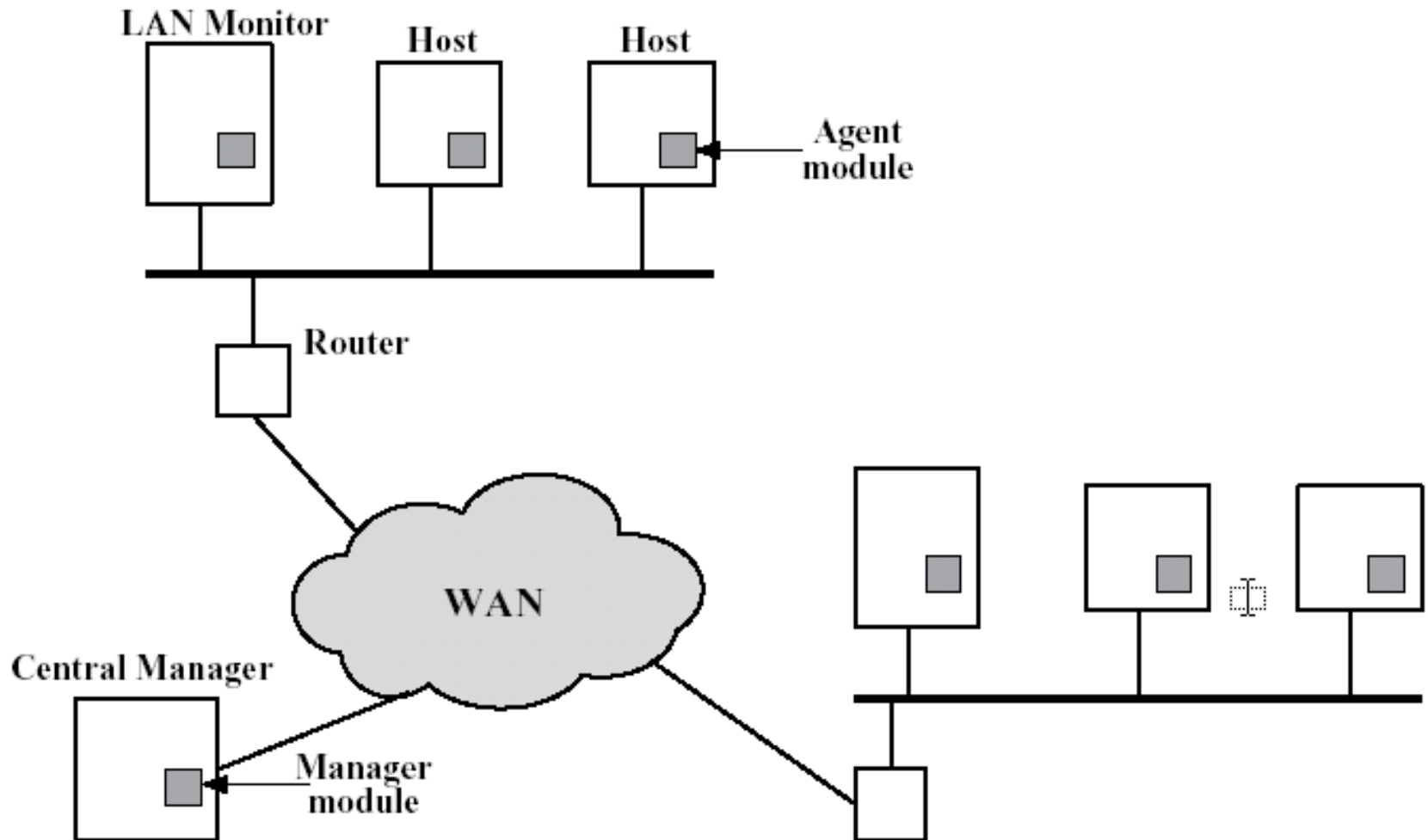
■ Rule-based detection

- ⊗ Involves attempt to define a set of rules that can be used to decide that a given behavior is that of an intruder

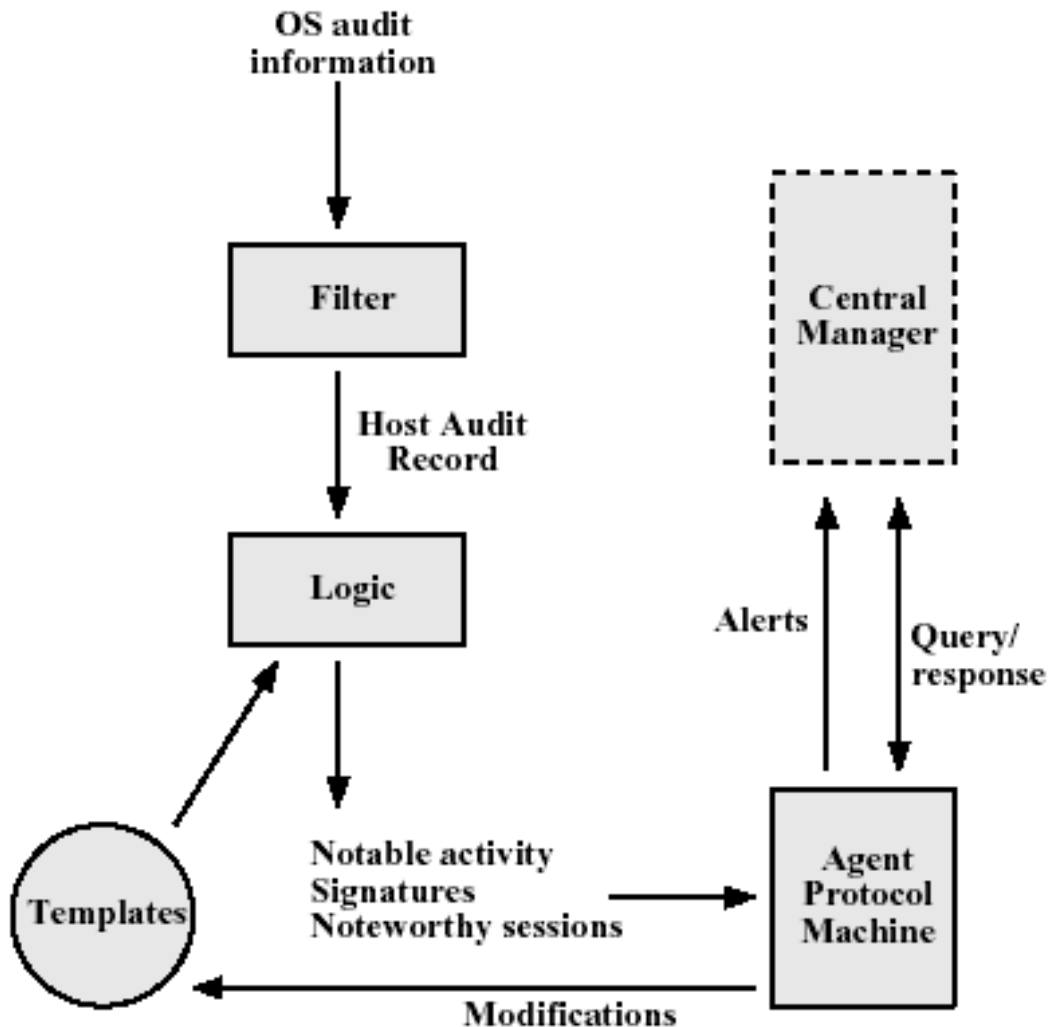
Distributed Intrusion Detection

- Computing resources are distributed now
- If all computing resources collaborate in intrusion detection – intrusion can be detected quickly

Architecture for Distributed Intrusion Detection



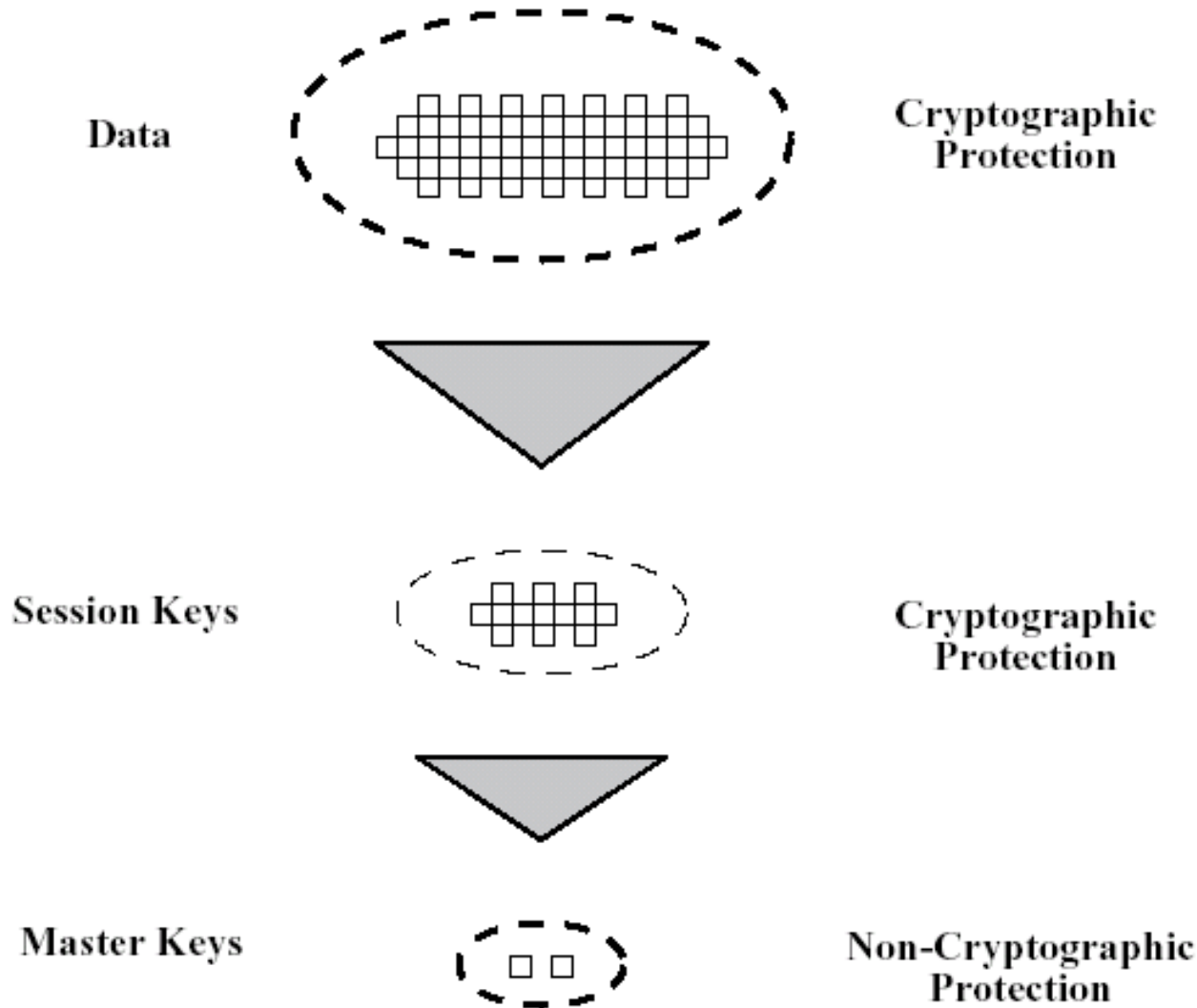
Agent Architecture



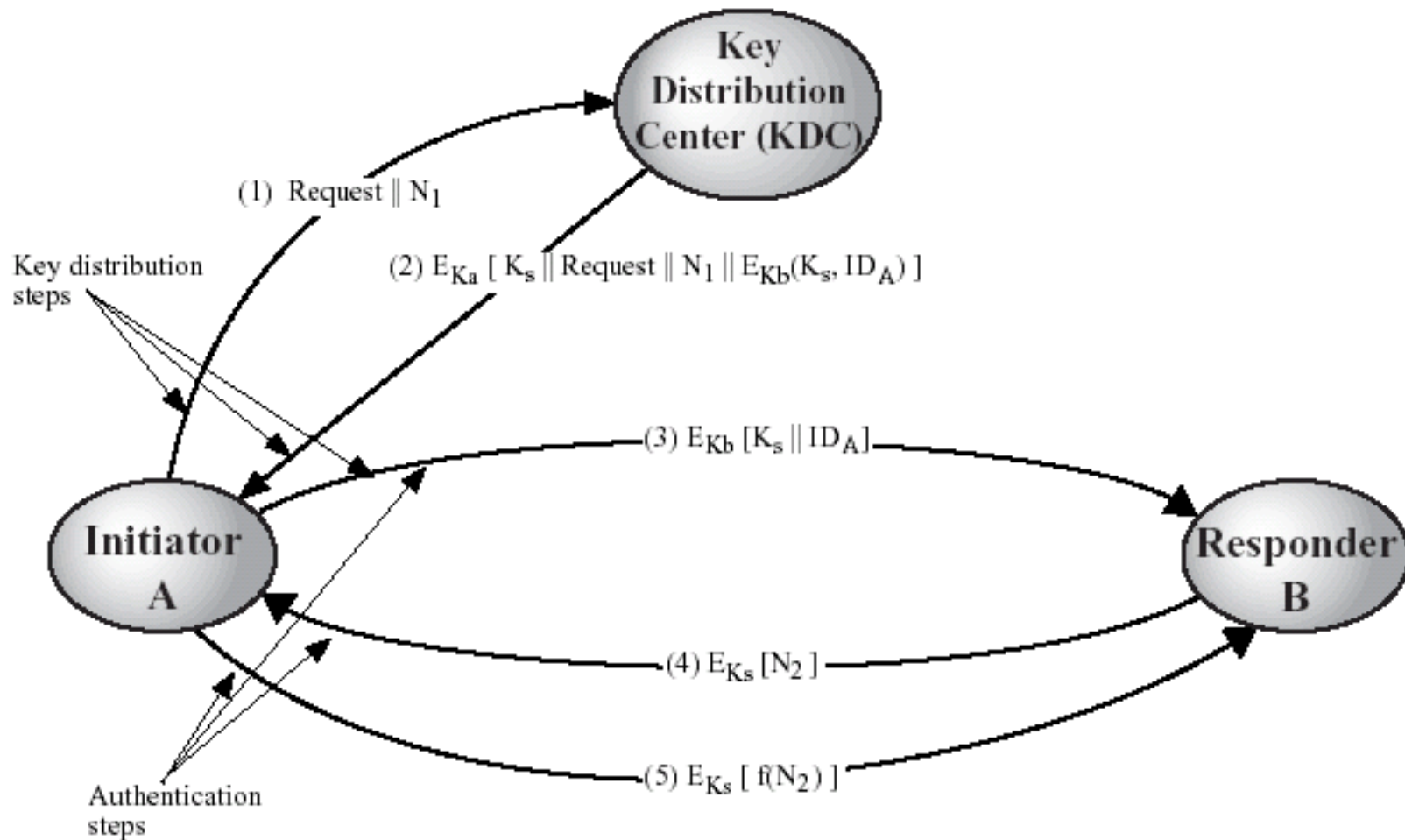
Key Management

- Issues related to keys:
- **Key Generation** – keys should be generated using CSPRNG
- **Key Storage** – keys must be stored securely
- **Key Distribution** – several approaches to exchange keys
 - ⊗ KDC – Key Distribution Centre – SKC-based solution
 - ⊗ Public Key protocol to exchange keys
- **Key lifetime and expiration**

The Use of a Key Hierarchy



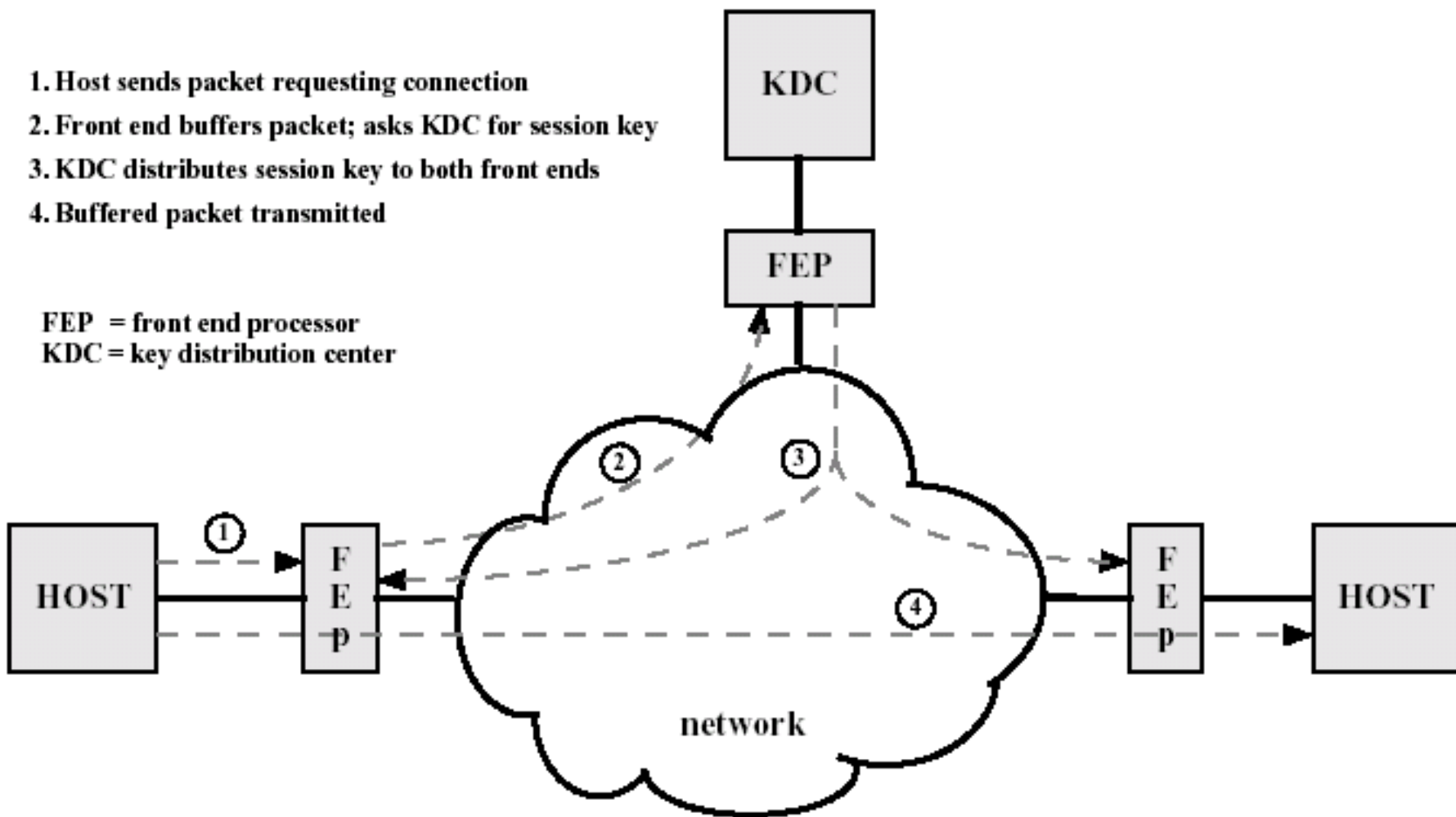
Key Distribution Scenario Using a KDC



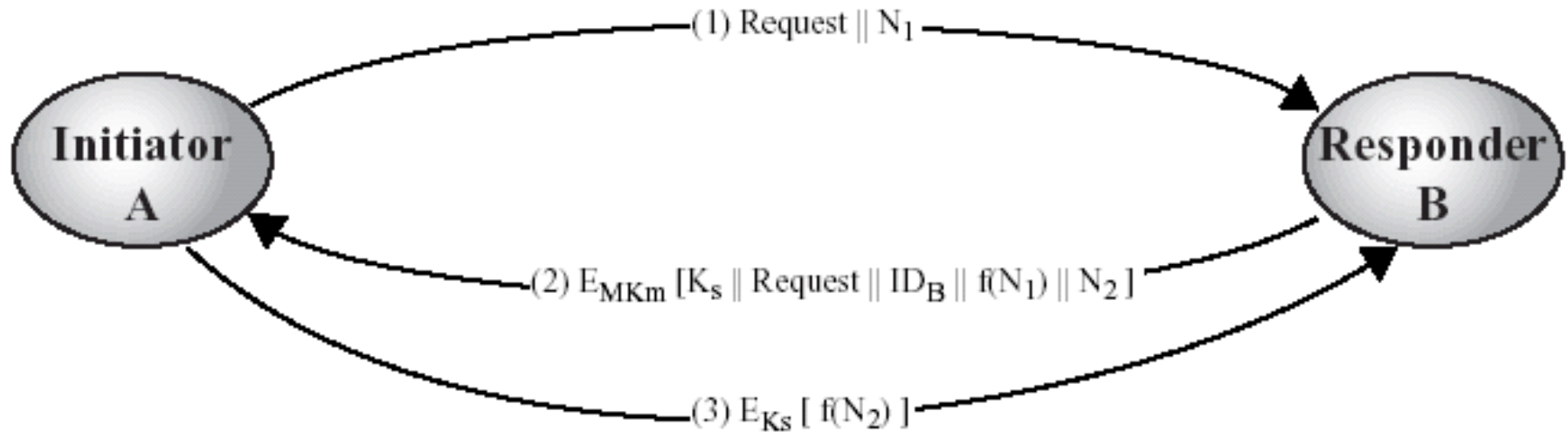
Automatic Key Distribution for Connection-Oriented Protocol

1. Host sends packet requesting connection
2. Front end buffers packet; asks KDC for session key
3. KDC distributes session key to both front ends
4. Buffered packet transmitted

FEP = front end processor
KDC = key distribution center



Decentralized Key Distribution



❑ Each user must already share a master key (K_m) with every other user

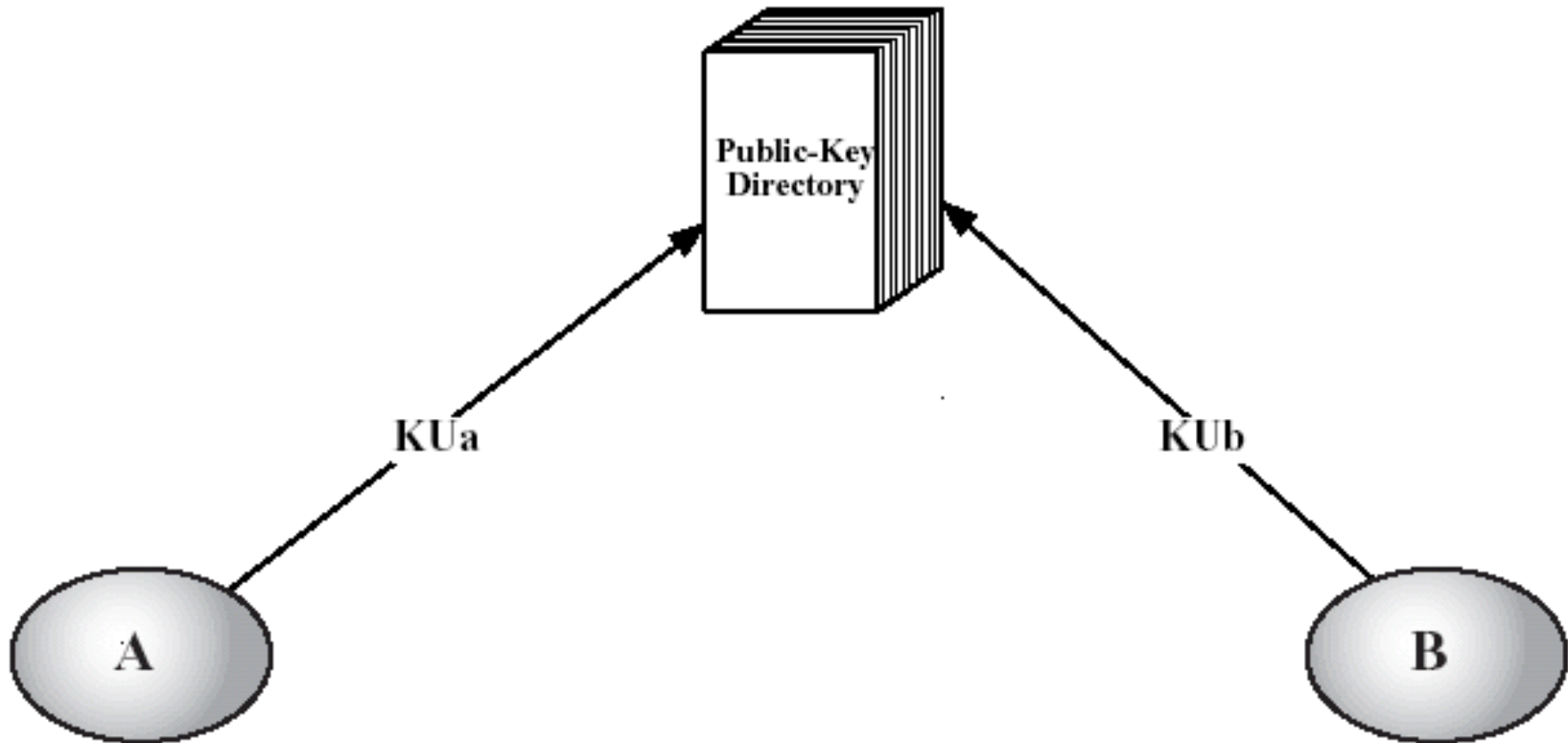
❑ Requires $[n(n - 1)]/2$ Master Keys for a system with n users

Uncontrolled Public Key Distribution



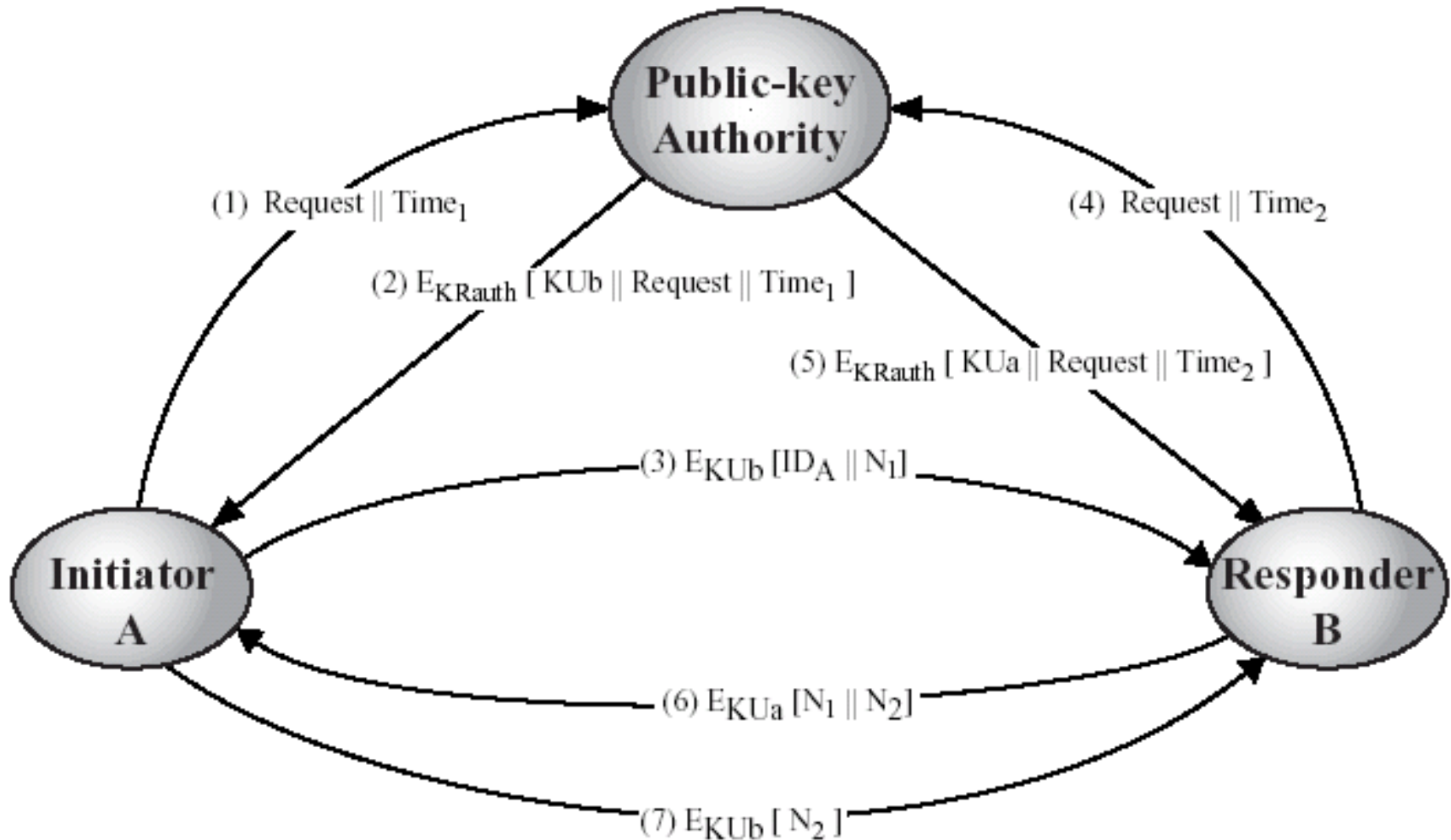
□ Users announce their Public Keys, publicly, such as in email messages or newsgroup postings

Public Key Publication

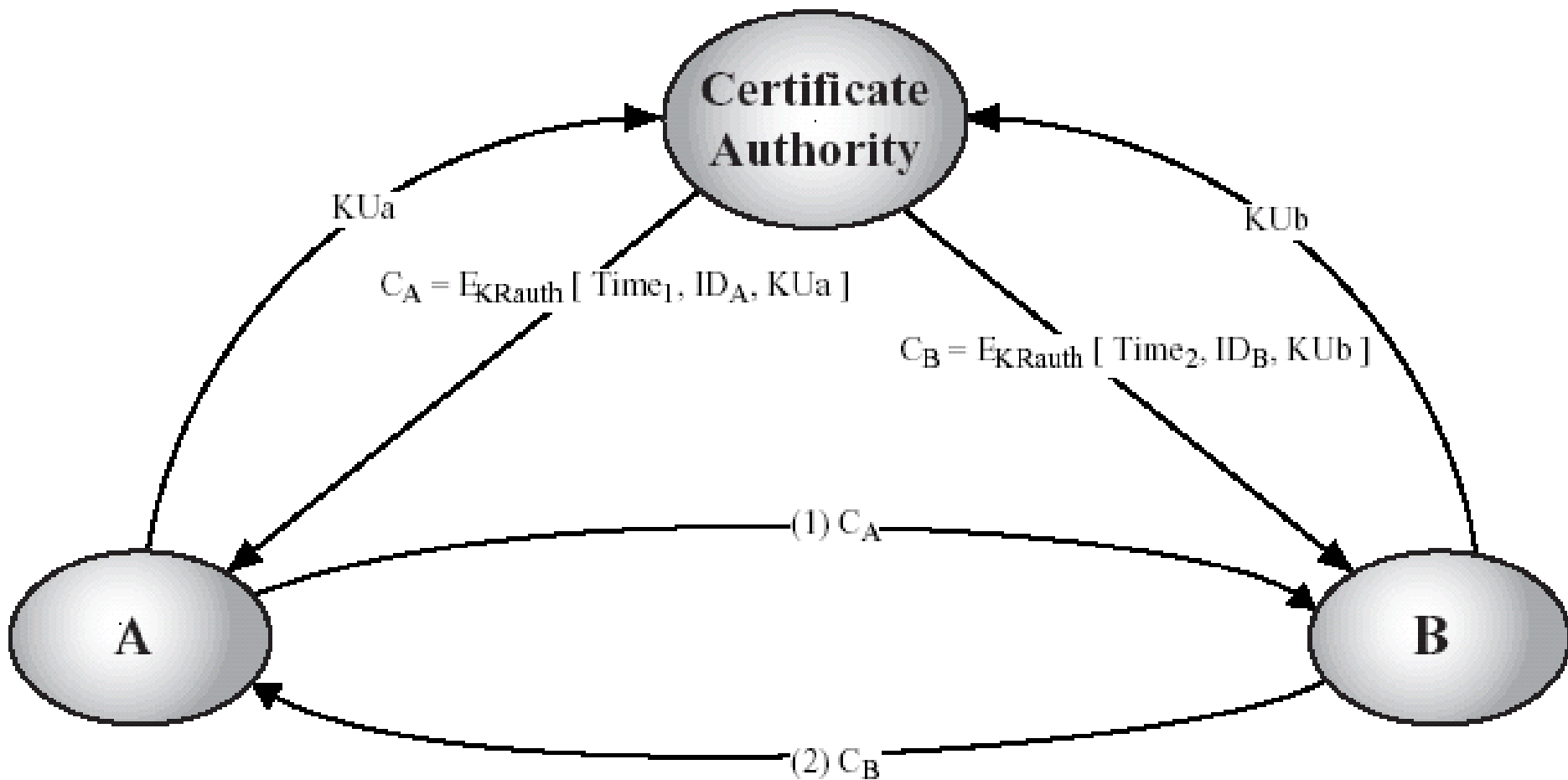


❑ Users publish their public keys in a globally accessible public-key directory

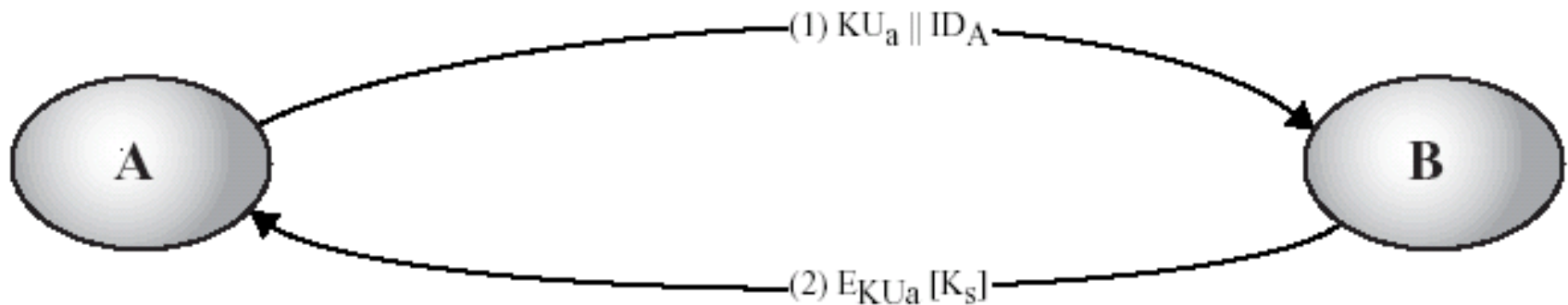
Public-Key Distribution Scenario



Exchange of Public-Key Certificates



Simple Use of Public-Key Encryption to Establish a Session Key



□ A first sends its Public key KU_a and then sends a session key K_s encrypted using that public key

□ This is susceptible to attack by a malicious active intruder in control of the communications channel

Public-Key Distribution of Secret Keys

