CS 194: Distributed Systems
Security

Scott Shenker and Ion Stoica
Computer Science Division
Department of Electrical Engineering and Computer Sciences
University of California, Berkeley
Berkeley, CA 94720-1776

Outline

- Key Management
- Group management
- Authorization management
- Example: Kerberos

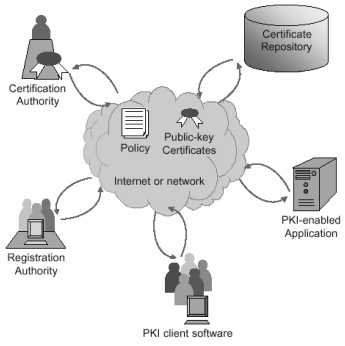
Security Management

- Problem: how do you get keys in the first place?
- Key distribution: securely associate an entity with a key
  - Example: Public Key Infrastructure (PKI)
- Key establishment: establish session keys
  - Use public key cryptography (we already know ho to do it)
  - Diffie-Hellman key exchange

Public Key Infrastructure **(PKI)**

- System managing public key distribution on a wide-scale
- Trust distribution mechanism
- Allow arbitrary level of trust

Components of a PKI

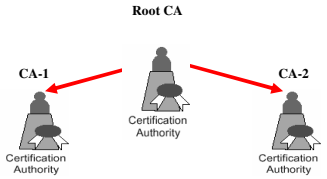


Digital Certificate

- Signed data structure that binds an entity (E) with its corresponding public key (K_E^+)
  - Signed by a recognized and trusted authority, i.e., Certification Authority (CA)
  - Provide assurance that a particular public key belongs to a specific entity
- How?
  - CA generates $K_{CA}^-(E, K_E^+)$
  - Everyone can verify signature using K_{CA}^+

Certification Authority (CA)

- People, processes responsible for creation, delivery and management of digital certificates
- Organized in an hierarchy (use delegation – see next)



7

Registration Authority

- People, processes and/or tools that are responsible for
  - Authenticating the identity of new entities (users or computing devices)
  - Requiring certificates from CA's.

8

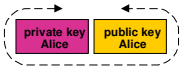
Certificate Repository

- A database which is accessible to all users of a PKI, contains:
  - Digital certificates,
  - Certificate revocation information
  - Policy information

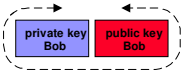
9

Example

- Alice generates her own key pair.



- Bob generates his own key pair.

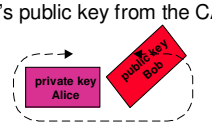


- Both sent their public key to a CA and receive a digital certificate

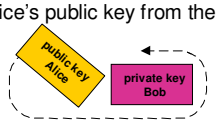
10

Example

- Alice gets Bob's public key from the CA



- Bob gets Alice's public key from the CA



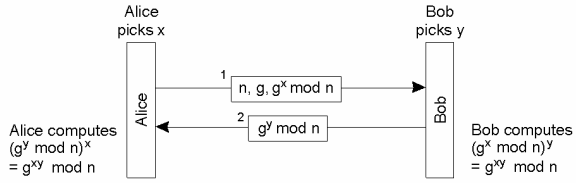
11

Certificate Revocation

- Process of publicly announcing that a certificate has been revoked and should no longer be used.
- Approaches:
  - Use certificates that automatically time out
  - Use certificate revocation list

12

Key Establishment: Diffie-Hellman Key Exchange



- Agree on two numbers n, g; both number can be made public!
- Alice and Bob pick two secret numbers x and y
- Similar to public-key cryptography
  - Example: For Alice, $K_A^- = x$, $K_A^+ = g^x \bmod n$

Outline

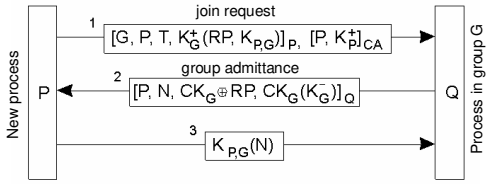
- Key Management
- Group management
- Authorization management
- Example: Kerberos

Secure Group Management

- Motivation: offer high availability for security services
- How: replicate services
- Problem: how to add a new replica to a group without compromising the integrity of the group?

Securely admitting a new group member

- C_{KG}: secret key used for communication within group
- K_G^+, K_G^-: public-private key pair to communicate with non-group members
- $K_{P,G}$: secret key
- RP: reply pad
- T: local time
- Notation: $[X]_Y$: X was signed by Y



Outline

- Key Management
- Group management
- Authorization management
- Example: Kerberos

Outline

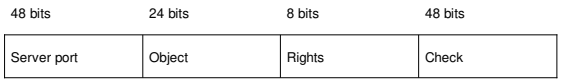
- Key Management
- Group management
- Authorization management
- Example: Kerberos

Authorization Management

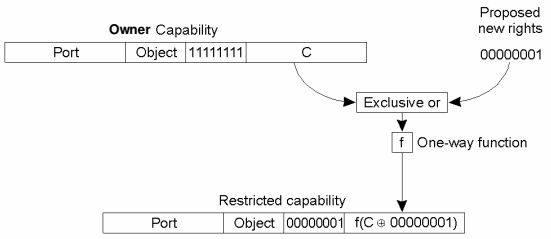
- Granting authorization rights
- Related with **access control** which **verifies** access rights (see book)

Capabilities (1)

- Capability:
  - Unforgeable data structure for a specific resource R
  - Specify access right the holder has with respect to R
- Capability in Amoeba:



Capabilities (2)



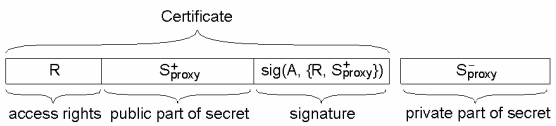
- Generation of a restricted capability from an owner capability

Delegation

- A wants to delegate an operation on a resource to B
- Problem: how does A delegates its access rights to B?
- Solutions: A signs (A, B, R)
- If B wants to delegate operation to C, C needs to contact A
  - Avoid this problem using a proxy (Neuman scheme)
  - Proxy: a token allowing its owner to operate with the same or rstricted rights as the entity granting the token

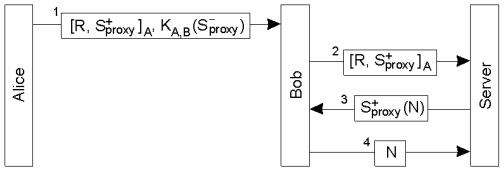
Delegation: Neuman Scheme

- The general structure of a proxy as used for delegation:



Delegation: Neuman Scheme

- Using a proxy to delegate and prove ownership of access rights
- In practice S^+_{proxy}, S^-_{proxy} can be a public-private key pair and N can be a nonce

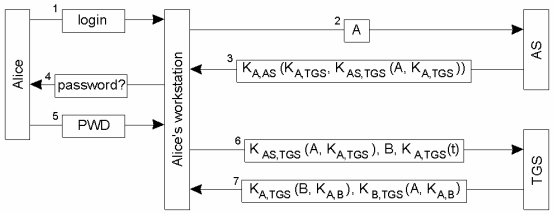


Kerberos

- Based on Needham-Schroeder authentication scheme
- Developed at MIT

25

Example: Kerberos

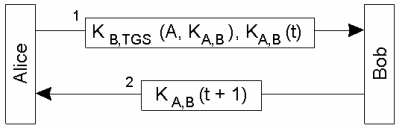


- Authentication in Kerberos
  - AS: Authentication server
  - TGS: Ticket Granting Service
  - T: timestamp used to avoid replay attacks of message 6

26

Example: Kerberos

- Setting up a secure channel in Kerberos:



27