**Key Management Review**

- Key management is where much security weakness lies
  - Choosing keys
  - Storing keys
  - Communicating keys

---

**Key Distribution**

- Conventional cryptography
  - Single key shared by both parties
- Public Key cryptography
  - Public key published to the world
    - Private key known only by owner
- Third party certifies or distributes keys
  - Certification infrastructure
  - Authentication

---

**Key Management Overview**

- Key size vs. data size
  - Affects security and usability
- Reuse of keys
  - Multiple users, multiple messages
- Initial exchange
  - The bootstrap/registration problem
  - Confidentiality vs. authentication

---

**Key Management Review**

- KDC’s
  - Generate and distribute keys
  - Bind names to shared keys
Key Management Overview

• Who needs strong secrets anyway
  – Users?
  – Servers?
  – The Security System?
  – Software?
  – End Systems?
• Secret vs. Public

Security Architectures

• DSSA
  – Delegation is the important issue
    • Workstation can act as user
    • Software can act as workstation
      – if given key
    • Software can act as developer
      – if checksum validated
  – Complete chain needed to assume authority
  – Roles provide limits on authority – new sub-
    principal

Group Key Management

• Group key vs. Individual key
  – Identifies member of groups vs.
    which member of group
  – PK slower but allows multiple
    verification of individuals

Group Key Management Issues

• Revoking access
  – Change messages, keys, redistribute
• Joining and leaving groups
  – Does one see old message on join
  – How to revoke access
• Performance issues
  – Hierarchy to reduce number of
    envelopes for very large systems
  – Hot research topic

Group Key Management Issues

• Revoking access
  – Change messages, keys, redistribute
• Joining and leaving groups
  – Does one see old message on join
  – How to revoke access
• Performance issues
  – Hierarchy to reduce number of
    envelopes for very large systems
  – Hot research topic