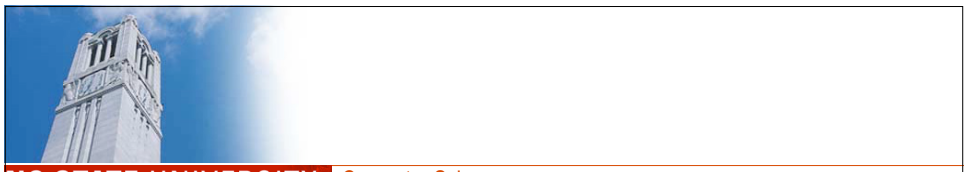


NC STATE UNIVERSITY Computer Science

CSC 474
Information Systems Security

Topic 3.1 Overview of Authentication

Authentication

- Authentication is the process of reliably verifying certain information.
- Examples
  - User authentication
    - Allow a user to prove his/her identity to another entity (e.g., a system, a device).
  - Message authentication
    - Verify that a message has not been altered without proper authorization.
- A related concept
  - identification

Identification

- *Identification* is a process through which one ascertains the identity of another person or entity.
- Authentication and identification are different.
  - Identification requires that the verifier check the information presented against all the entities it knows about,
  - Authentication requires that the information be checked for a single, previously identified, entity
  - Identification must, by definition, uniquely identify a given entity,
  - Authentication does not necessarily require uniqueness.

Authentication Mechanisms

- Password-based authentication
  - Use a secret quantity (the password) that the prover states to prove he/she knows it.
  - Threat: password guessing/dictionary attack

Authentication Mechanisms (Cont'd)

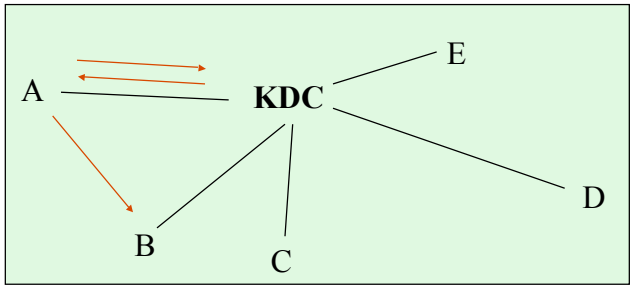
- Address-based authentication
  - Assume the identity of the source can be inferred based on the network address from which packets arrive.
  - Adopted early in UNIX and VMS
- Berkeley *rtools* (*rsh*, *rlogin*, etc)
  - */etc/hosts.equiv* file
    - List of computers
  - Per user *.rhosts* file
    - List of <computer, account>
- Threat
  - Spoof of network address
    - Not authentication of source addresses

Authentication Mechanisms (Cont'd)

- Cryptographic authentication protocols
  - Basic idea:
    - A prover proves some information by performing a cryptographic operation on a quantity that the verifier supplies.
  - Usually reduced to the knowledge of a secret value
    - A symmetric key
    - The private key of a public/private key pair

Trusted Intermediaries

- Problem: authentication for large networks
- Key Distribution Center (KDC)
  - Secret key cryptography



Disadvantages: high risk; single point of failure; performance bottleneck

Trusted Intermediaries

- Certification Authorities (CAs)
  - Public key cryptography
- Certificates
  - Signed messages that specify an identity and the corresponding public key
  - Signed with the well-known public key of a CA

CAs (Cont'd)

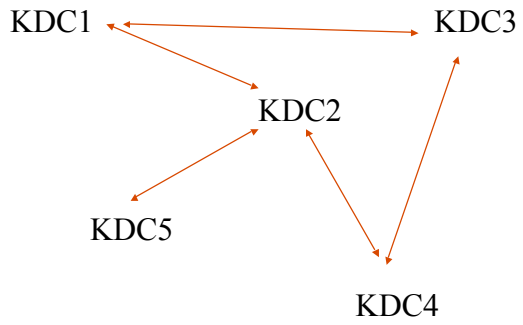
- Advantages
  - Doesn't have to be online
  - Lower risk compared with KDCs
  - Allow the network to operate even if CAs crash
  - Certificates can be public
  - A Compromised CA cannot decrypt previously secured traffic

CAs (Cont'd)

- Certificate revocation
  - Problem: how to deal with revoked certificates (before they expire)
  - Certificate Revocation List (CRL)
    - List of revoked certificates
  - Timely and reliable distribion of CRLs is a critical and difficult problem.

Multiple Trusted Intermediaries

- Multiple KDC domains
  - KDCs share keys between each other



Multiple Trusted Intermediaries (Cont'd)

- Multiple CA domains
  - CAs issue certificates to each other