Authentication Protocols

CSCI 454/554

Authentication

- Identity Authentication
  - Password-based: vulnerable to eavesdropping
  - Occupancy of master keys or shared-secret
  - Public-key certificate

- Authenticated key exchange
Authentication (Key) Protocols

- used to convince parties of each others identity and to exchange session keys
- may be one-way or mutual
- key issues are
  - confidentiality – to protect session keys
  - timeliness – to prevent replay attacks

Replay Attacks

- where a valid signed message is copied and later resent
  - simple replay
  - repetition that can be logged
  - repetition that cannot be detected
  - backward replay without modification
- countermeasures include
  - timestamps (needs synchronized clocks)
  - challenge/response (using unique nonce)
Using Symmetric Encryption

- usually with a trusted Key Distribution Center (KDC)
  - each party shares own master key with KDC
  - KDC generates session keys used for connections between parties
  - master keys used to distribute these to them
- Needham-Schroeder Protocol
  - step 3 is vulnerable to a replay attack if an old session key has been compromised

Replay Attack

3. A$\rightarrow$B: $E_{K_h}[K_s||ID_A]$
   Eve intercept it, and reply with old session key $K'$
3'. Eve$\rightarrow$B: $E_{K_h}[K's||ID_A]$: replay old message
4. B$\rightarrow$A: $E_{K's}[N_2]$
   Eve intercept it, and impersonate A’s response
5. E $\rightarrow$B: $E_{K's}[\overline{f}(N_2)]$

B thought that he is communicate with A, but after step 3 he is exchanging messages with Eve.
Timestamp (Denning)

1. A→KDC: $ID_A \parallel ID_B$
2. KDC→A: $E_{Ka}\{ID_B\parallel K_s\parallel T_c\parallel E_{Kb}\{ID_A\parallel K_s\parallel T_c\}\}$
3. A→B: $E_{kb}\{ID_A\parallel K_s\parallel T_c\}$
4. B→A: $E_{Ks}[N_2]$
5. A→B: $E_{Ks}[f(N_2)]$

A and B verify timeliness: $|\text{clock} - T_c| < \Delta t$

- Requiring clock synchronization, otherwise
  - Suppress-replay attacks

Nonce (Neumann)

- Handshake: challenge and response
  - response binds the nonce with the session key and be encrypted

A———>B———>KDC———>A

B———>KDC———>A———>B
Neumann Protocol

1. A→B: \( ID_A \parallel N_a \)
2. B→KDC: \( ID_B \parallel N_b \parallel E_{K_b}[ID_A \parallel N_a \parallel \text{TTL}] \)
3. KDC→A: \( E_{K_a}[ID_B \parallel N_a \parallel K_s] \parallel E_{K_b}[ID_A \parallel K_s \parallel \text{TTL}] \parallel N_b \)
4. A→B: \( E_{K_s}[N_b] \parallel E_{K_b}[ID_A \parallel K_s \parallel \text{TTL}] \)

- \( E_{K_b}[ID_A \parallel K_s \parallel \text{TTL}] \) used as ticket by A later
- without contacting with KDC.

Neumann Protocol (Con’t)

1. A→B: \( E_{K_b}[ID_A \parallel K_s \parallel \text{TTL}] \parallel N'_a \)
2. B→A: \( N'_b \parallel E_{K_b}[N'_a] \)
3. A→B: \( E_{K_s}[N'_b] \)

- At step 1, B verifies the ticket has not expired
Using Public-Key Encryption

- have a range of approaches based on the use of public-key encryption
- have public keys of other parties

1. \( A \rightarrow B: E_{K+b}[ID_A \ || \ N_a] \)
2. \( B \rightarrow A: E_{K+a}(E_{K-b}[K_s] || N_a || N_b) \)
3. \( A \rightarrow B: E_{K+b}[N_b] \)

Others’ Public Key Not Available

- using a central Authentication Server (AS)
  - distribute the public keys
  - everyone knows AS’s public key
- various protocols exist using timestamps or nonces
  - Timestamps (Denning81)
  - Nonces (Woo and Lam92)
Denning AS Protocol

- Denning 81 presented the following:
  1. $A \rightarrow AS: ID_A || ID_B$
  2. $AS \rightarrow A: E_{K-as}[ID_A||K^+_a||T] || E_{K-as}[ID_B||K^+_b||T]$
  3. $A \rightarrow B: E_{K-as}[ID_A||K^+_a||T] || E_{K-as}[ID_B||K^+_b||T] || E_{K^+_b}[E_{K-as}[K_a||T]]$

- session key is chosen by $A$, hence $AS$ need not be trusted to protect it
- timestamps prevent replay but require synchronized clocks

One-Way Authentication

- required when sender & receiver are not in communications at same time (eg. email)
- have header in clear so can be delivered by email system
- may want contents of body protected & sender authenticated
Using Symmetric Encryption

- can refine use of KDC but can’t have final exchange of nonces:
  1. $A \rightarrow KDC: ID_A \ || \ ID_B \ || \ N_I$
  2. $KDC \rightarrow A: E_{K_a}[Ks \ || \ ID_B \ || \ N_I \ || \ E_{K_b}[Ks||ID_A]]$
  3. $A \rightarrow B: E_{K_h}[Ks||ID_A] \ || \ E_{K_s}[M]$
- does not protect against replays
  - could rely on timestamp in message, though email delays make this problematic

Public-Key Approaches

- if confidentiality is major concern, can use:
  $A \rightarrow B: E_{K+a}[Ks] \ || \ E_{K_s}[M]$
  - has encrypted session key, encrypted message
- if authentication needed use a digital signature:
  $A \rightarrow B: M \ || \ E_{K-a}[H(M)]$

$A \rightarrow B: E_{K_s}\{M \ || \ E_{K-\alpha}[H(M)]\} \ || \ E_{K+b}[Ks]$