AUTHENTICATION (II)

Authentication of People

Security Handshakes

Authentication of People

- What you know – Password
- What you have – Authentication token
- What you are – Biometrics

Passwords

- Vulnerable to dictionary attack
- Vulnerable to eavesdropping
- Typical password information is 2 bits per character
- Would need 32 characters to be ≡ 64-bit key
- Enforced password change has limited value

Protection against dictionary attack

- Efficient attack would hash complete dictionary and compare to contents of store of hashed passwords
- Protect by associating random number ("salt") with user
- Store hash (password salt)

Trojan Horse Password Attack

- Attacker leaves rogue program running on machine which displays login prompt
- When user name / password are entered program terminates (in a non-suspicious way)
- Valid user name / password pairs are collected

Protection against Trojan Horse

- Design real login prompt with different protocol to general data input
- Design screen protocol to prevent login emulation
- Precede real login with program interrupt command (e.g. Ctrl – Alt – Del in Windows)

Authentication Tokens

- Traditional keys
  - easy to reproduce
- Magnetic stripe cards
  - more information but easy to copy
  - offline authentication by hash (key PIN)
- Smart cards
  - difficult to copy
  - capable of security conversation with reader

Smart Cards

- PIN protected memory card
- Cryptographic challenge / response cards
- Cryptographic calculators

Biometric Devices

- Retinal Scanner
- Fingerprints
- Face recognition
- Iris Scanner
- Handprints
- Voiceprints
- Keystroke timing
- Signatures

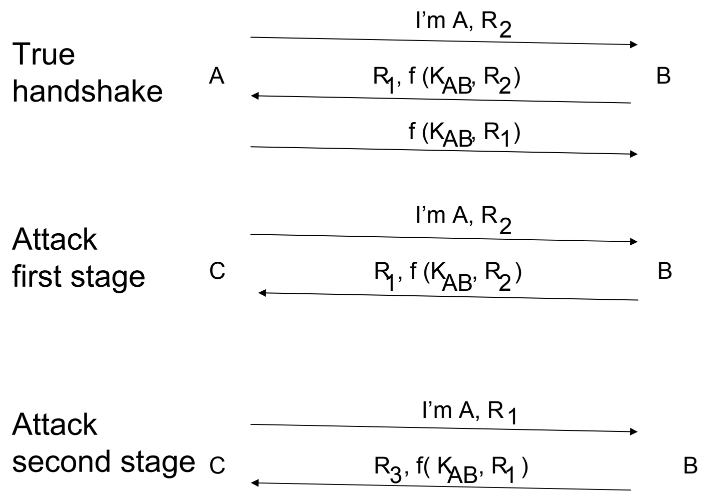
Issues with Biometric Devices

- User objections
- Probability false acceptance/false rejection
- False rejection may be reduced at expense of higher false acceptance

Security Handshakes

- Login
- Data Integrity/Encryption
- Mediated Authentication

Reflection Attack

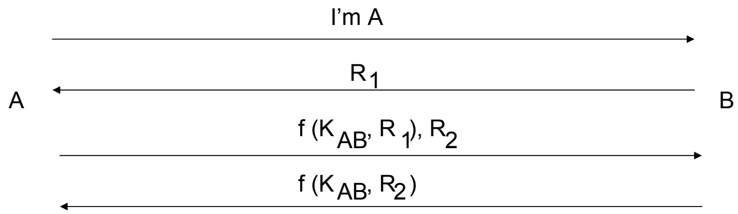


Protection against reflection attack

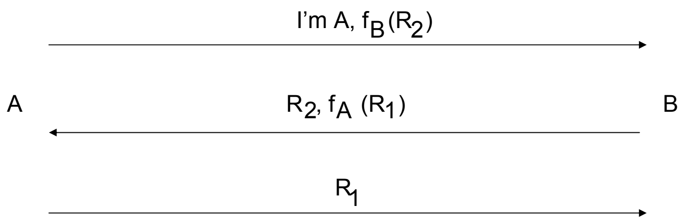
- A could authenticate B using a different shared key from which B authenticates A
- A could use a different type of challenge to that used by B (e.g. A could use even numbers and B could use odd)

Protection against password guessing

C could impersonate A and obtain an R , f (K_{AB} R) with which it could do a search to find K . Protection by adding extra message to handshake

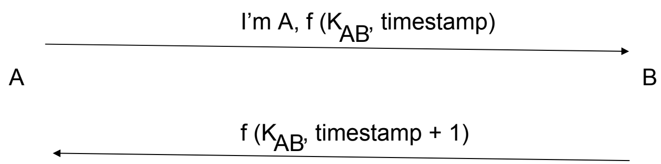


Public Keys



$f_A(.)$ and $f_B(.)$ are encryptions using public keys of A and B respectively

Timestamps



Integrity/Encryption of Data

- Shared secret
- Public keys
- One – way public key

Shared Secret for session key establishment

- Form session key from K_{AB} and R
- e.g. f (K_{AB}+ 1 R)
- should not use f (K_{AB} R) or f (K_{AB} R + 1)

Public key exchange for session key establishment

- A chooses random number and encrypts with B's public key – vulnerable to impersonation
- As above but signed with A's private key
- A and B both choose random numbers R_1 and R_2 and exchange encrypted under each other's public keys. Session key is $R_1 \oplus R_2$
- Signed Diffie-Hellman key exchange

One – Way Public key for Session Key Establishment

- A sends random number R encrypted under B's public key
- Diffie-Hellman key exchange signed in only one direction

Mediated Authentication Needham-Schroeder