Authentication & Identification

SSL and S-HTTP

- SSL (Secure Socket Layer), S-HTTP (Secure HTTP)
- Certificate based systems without specific PKI
- CA certificates are embedded in browsers
- You (client) trust them because the browser company (MS, NS, AOL) wants you to!
- The worst security, but the most practical !!!
Authentication and identification

Purpose

Examples:
- Bank transactions, e.g., cash withdrawals
- Remote login
- File access or print

Has user’s secrets

Send secret or prove knowing it?

TTP

Peer Or Server

Doesn't
Human Failings

- Humans are notoriously unreliable
- Human memory is very volatile storage

What a human can remember:
- PIN (not more than 6-8 digits)
- Password (a word or a short phrase)
- Single-digit sums? Forget it…

Biometrics:
Eyes, fingers, writing, toes?

Concrete ID Scenarios

- PIN-, PW-, Biometric-based schemes
  - Kerberos (covered later)
  - SecureID token
  - Iris/retina scanners
  - Thumbprint & Handprint
  - Handwriting acceleration & pressure
- Public Key Identification Schemes:
  - Fiat-Shamir, Schnorr, Guillou-Quisqater
SecureID

TTP knows all secrets!

Fiat-Shamir ID Scheme

\[ p, q \text{ -- large primes} \]
\[ n = pq \]
\[ t \text{ -- security parameter} \]

Publics: \( n, t, \text{ID} = x^2 \mod n \)

Secrets: \( p, q \text{ -- global}, x \text{ -- Alice} \)

Note: \( \gcd(x, n) = 1 \)

1. Alice: \( k \in [1, n], w = k^2 \mod n \)
2. Bob: \( r \in [0, 1] \)
3. Alice: \( y = kr \mod n \)
4. Bob: \( y^2 \equiv wID \mod n \)

Repeat \( t \) times!
Fiat-Shamir ID Scheme

$p, q$ – large primes

$n = pq$

$t$ – security parameter

Publics: $n, t, ID = x^2 \mod n$

Secrets: $p, q$ – global, $x$ – Alice

Note: $\gcd(x, n) = 1$

1. Alice: $k \in [1,n]$, $w = k^2 \mod n$

2. Bob: $r \in [0,1]$

3. Alice: $y = k^r \mod n$

4. Bob: $y^2 = w^{ID} \mod n$

Repeat $t$ times!

Suppose $t=1$

Eve chooses:

- any $k$
- $w = k^2 / ID$
- if $(r = 1) y = k$
- $Bob: y^2 \equiv k^2 = w^{ID} = k^2$
- if $(r = 0) y = \sqrt{w} = k / \sqrt{ID}$

Schnorr ID Scheme (contd)

$p$ – large prime

$q$ – large prime divisor of $p - 1$

$g$ – generator

$a = g^{(p-1)/q} \mod p$

$t$ – security parameter (40?)

Publics: $p, q, g, a, t, ID = a^{-x} \mod p$

Secrets: $x$ (Alice)

Alice: $k \in [0, q]$, $w = a^k \mod p$

Bob: $r \in [1, 2^t]$

Alice: $y = k + xr \mod q$

Bob: $w = ? = a^{ID} \mod p$

$w' = a^y ID^r = a^{y-xr}$
Attacks on ID Schemes

- Eve forges Alice’s certificate
- Eve guesses Bob’s challenge
- Eve computes $x$ from ID
- Eve obtains a copy-cat certificate?

- Efficient for BW, CPU
- Targeted for smartcards (Alice)
- Used commercially
- Not proven secure