Authentication

- Entity Authentication (Identification)
  - Over the communication network, one party, Alice, shows to another party, Bob, that she is the real Alice.
  - Authenticate an entity by presenting some identification information
  - Should be secure against various attacks
  - Through an interactive protocols using secret information

- Message Authentication
  - Show that a message was generated by an entity
  - Using digital signature or MAC
## Classification of Identification

<table>
<thead>
<tr>
<th>Method</th>
<th>Examples</th>
<th>Reliability</th>
<th>Security</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>What you Remember (know)</strong></td>
<td>Password Telephone # Reg. #</td>
<td>M/L</td>
<td>M (theft) L (impersonation)</td>
<td>Cheap</td>
</tr>
<tr>
<td><strong>What you have</strong></td>
<td>Registered Seal Magnetic Card</td>
<td>M</td>
<td>L (theft) M (impersonation)</td>
<td>Reasonable</td>
</tr>
<tr>
<td><strong>What you are</strong></td>
<td>Bio-metric (Fingerprint, Eye, DNA, face, Voice, etc)</td>
<td>H</td>
<td>H (theft) H (Impersonation)</td>
<td>Expensive</td>
</tr>
</tbody>
</table>
Identification Schemes

- Password-based scheme (weak authentication)
  - `crypt passwd` under UNIX
  - one-time password
- Challenge-Response scheme (strong authentication)
  - Symmetric cryptosystem
  - MAC (keyed-hash) function
  - Asymmetric cryptosystem
- Using Cryptographic Protocols
  - Fiat-Shamir identification protocol
  - Schnorr identification protocol, etc
Identification by Password

Prover

 passwd, A

Veriﬁer

 passwd table

A h(passwd)

 passwd

h

y

= n

accept

reject

Sniffing attack
Replay attack - Static password
S/Key (One-Time Password System)

**Initial Setup**

1. login ID
2. N
3. compute \( f^N(S) = X_N \)
4. \( X_N \)
5. compute \( f(X_N) = X_{N+1} \)
6. compare
7. store

**Client**

- Hash function \( f() \)
- pass-phrase \( S \)

**Host**

- Hash function \( f() \)
- pass-phrase \( S \)
- compute \( f(S), f(f(S)), \ldots, X_1, X_2, X_3, \ldots, X_N \)
- store \( X_{N+1} \)
Bio-identification
Biometric Recognition System

- False accept rate (FAR): Proportion of imposters accepted
- False reject rate (FRR): Proportion of genuine users rejected
- Failure to enroll rate (FTE): Portion of population that cannot be enrolled
- Failure to acquire rate (FTA): Portion of population that cannot be verified
Biometric Recognition System

- False accept rate (FAR): Proportion of imposters accepted
- False reject rate (FRR): Proportion of genuine users rejected
- Failure to enroll rate (FTE): Portion of population that cannot be enrolled
- Failure to acquire rate (FTA): Portion of population that cannot be verified
Fake Fingerprint

Access was granted 75% of the time using gummy fingers
Applications

**Goal:** Automatic & reliable person identification in unattended mode, often remotely

- Iris matching: Heathrow Airport
- US-VISIT Program
- Cellular phone: Siemens
- Grocery store payment: Indivos
- Automobile: Audi A8
- Disney World