Authentication

- Basics
- Passwords
- Challenge-Response
- Biometrics
- Location
- Multiple Methods
Pass Algorithms

- Challenge-response with the function $f$ itself a secret
  - Example: Use in combination with a standard password scheme
    - User enters password
    - Display second login screen
    - Challenge is a random string of characters such as “abcdefg”, “ageksido”
    - Response is some function of that string such as “bdf”, “gkip”
    - Only authorized users know how to respond to the challenge
- Can alter algorithm based on ancillary information
  - Network connection is as above, dial-up might require “aceg”, “aesd”
One-Time Passwords

- Password that can be used exactly once
  - After use, it is immediately invalidated
- Challenge-response mechanism
  - Challenge is number of the authentication attempt; response is password for that particular number
- Problems
  - Synchronization of user, system
  - Generation of good random passwords
  - Password distribution problem
S/Key

- One-time password scheme based on idea of Lamport
- $h$ one-way hash function (MD5 or SHA-1, for example)
- User chooses initial seed $k$
- System calculates:
  \[ h(k) = k_1, \ h(k_1) = k_2, \ldots, \ h(k_{n-1}) = k_n \]
- Passwords are reverse order:
  \[ p_1 = k_n, \ p_2 = k_{n-1}, \ldots, \ p_{n-1} = k_2, \ p_n = k_1 \]
S/Key Protocol

System stores maximum number of authentications $n$, number of next authentication $i$, last correctly supplied password $p_{i-1}$.

System computes $h(p_i) = h(k_{n-i+1}) = k_{n-i} = p_{i-1}$. If match with what is stored, system replaces $p_{i-1}$ with $p_i$ and increments $i$. 
Hardware Support

- **Token-based**
  - Used to compute response to challenge
    - May encipher or hash challenge
    - May require PIN from user

- **Temporally-based**
  - Every minute (or so) different number shown
    - Computer knows what number to expect when
  - User enters number and fixed password
RSA SecurID

Two-Factor Authentication

With something you know—a PIN, just like your ATM.

1  2  3
4  5  6
7  8  9
0

http://www.rsa.com/node.aspx?id=1159
Biometrics

- Automated measurement of biological, behavioral features that identify a person
  - Fingerprints: optical or electrical techniques
    - Maps fingerprint into a graph, then compares with database
    - Measurements imprecise, so approximate matching algorithms used
  - Voices: speaker verification or recognition
    - Verification: uses statistical techniques to test hypothesis that speaker is who is claimed (speaker dependent)
    - Recognition: checks content of answers (speaker independent)
Other Characteristics

- Can use several other characteristics
  - Eyes: patterns in irises unique
    - Measure patterns, determine if differences are random; or correlate images using statistical tests
  - Faces: image, or specific characteristics like distance from nose to chin
    - Lighting, view of face, other noise can hinder this
  - Keystroke dynamics: believed to be unique
    - Keystroke intervals, pressure, duration of stroke, where key is struck
    - Statistical tests used
Cautions

• These can be fooled!
  • Assumes biometric device accurate \textit{in the environment it is being used in}!
  • Transmission of data to validator is tamperproof, correct
Location

- If you know where user is, validate identity by seeing if person is where the user is
  - Requires special-purpose hardware to locate user
    - GPS (global positioning system) device gives location signature of entity
    - Host uses LSS (location signature sensor) to get signature for entity
Multiple Methods

- Example: “where you are” also requires entity to have LSS and GPS, so also “what you have”
- Can assign different methods to different tasks
  - As users perform more and more sensitive tasks, must authenticate in more and more ways (presumably, more stringently)