CS 356 – Lecture 5
User Authentication

Spring 2013
Review

• Chapter 1: Basic Concepts and Terminology
  – Integrity, Confidentiality, Availability, Authentication, and Accountability
  – Types of threats: active vs. passive, insider/outsider
  – Lots of terminology and general concepts

• Chapter 2: Basic Cryptographic Tools
  – Symmetric key encryption and secure hashing
  – Public key cryptography
  – Random Numbers

• Chapter 3 – User Authentication
  – Password
Chapter 3

User Authentication
## Types of Cards Used as Tokens

<table>
<thead>
<tr>
<th>Card Type</th>
<th>Defining Feature</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embossed</td>
<td>Raised characters only, on front</td>
<td>Old credit card</td>
</tr>
<tr>
<td>Magnetic stripe</td>
<td>Magnetic bar on back, characters on front</td>
<td>Bank card</td>
</tr>
<tr>
<td>Memory</td>
<td>Electronic memory inside</td>
<td>Prepaid phone card</td>
</tr>
<tr>
<td>Smart Contact</td>
<td>Electronic memory and processor inside</td>
<td>Biometric ID card</td>
</tr>
<tr>
<td>Contactless</td>
<td>Electrical contacts exposed on surface</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Radio antenna embedded inside</td>
<td></td>
</tr>
</tbody>
</table>
Memory Cards

- can store but do not process data
- the most common is the magnetic stripe card
- can include an internal electronic memory
- can be used alone for physical access
  - hotel room
  - ATM
- provides significantly greater security when combined with a password or PIN
- drawbacks of memory cards include:
  - requires a special reader
  - loss of token
  - user dissatisfaction
Smartcard

- physical characteristics:
  - include an embedded microprocessor
  - a smart token that looks like a bank card
  - can look like calculators, keys, small portable objects

- interface:
  - manual interfaces include a keypad and display for interaction
  - electronic interfaces communicate with a compatible reader/writer

- authentication protocol:
  - classified into three categories: static, dynamic password generator and challenge-response
Smart Card Dimensions

The smart card chip is embedded into the plastic card and is not visible. The dimensions conform to ISO standard 7816-2.

Typical chip layout:

- RAM
- EEPROM
- ROM
- CPU
- Crypto coprocessor

Dimensions:
- Width: 85.6 mm
- Height: 54 mm
Communication Initialization between a Smart Card and a Reader

- Figure 3.4 Communication Initialization between a Smart Card and a Reader
- Source: Based on [TUNS06].

ATR = Answer to reset
PTS = Protocol type selection
Biometric Authentication

- attempts to authenticate an individual based on unique physical characteristics
- based on pattern recognition
- is technically complex and expensive when compared to passwords and tokens

physical characteristics used include:
- facial characteristics
- fingerprints
- hand geometry
- retinal pattern
- iris
- signature
- voice
Cost Versus Accuracy

Figure 3.5 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.
Operation of a Biometric System

Figure 3.6 A Generic Biometric System Enrollment creates an association between a user and the user’s biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.
Figure 3.7 Profiles of a Biometric Characteristic of an Imposter and an Authorized User. In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value \( (s) \) is greater than a preassigned threshold \( (f) \), a match is declared.
Figure 3.8 Idealized Biometric Measurement Operating Characteristic Curves. Different biometric application types make different trade-offs between the false match rate and the false nonmatch rate. Note that system A is consistently inferior to system B in accuracy performance. [JAIN00]
Remote User Authentication

- **authentication over a network, the Internet, or a communications link is more complex**
  - additional security threats such as:
    - eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- **generally rely on some form of a challenge-response protocol to counter threats**
**Password Protocol**

- **Example of a challenge-response protocol**

<table>
<thead>
<tr>
<th>Client</th>
<th>Transmission</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U$, user</td>
<td>$U \rightarrow$</td>
<td>random number $h(), f()$, functions</td>
</tr>
<tr>
<td>$P'$ password</td>
<td>$\leftarrow {r, h(), f()}$</td>
<td></td>
</tr>
<tr>
<td>$r'$, return of $r$</td>
<td>$f(r', h(P')) \rightarrow$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$\leftarrow \text{yes/no}$</td>
<td>if $f(r', h(P')) = f(r, h(P(U)))$ then yes else no</td>
</tr>
</tbody>
</table>

(a) Protocol for a password

- **user transmits identity to remote host**
- **host generates a random number (nonce)**
- **nonce is returned to the user**
- **host stores a hash code of the password**
- **function in which the password hash is one of the arguments**
- **use of a random number helps defend against an adversary capturing the user’s transmission**
Token Protocol

- user transmits identity to the remote host
- host returns a random number and identifiers
- token either stores a static passcode or generates a one-time random passcode
- user activates passcode by entering a password
- password is shared between the user and token and does not involve the remote host

<table>
<thead>
<tr>
<th>Client</th>
<th>Transmission</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U, \text{user}$</td>
<td>$U \rightarrow$</td>
<td>$r$, random number $h(), f()$, functions</td>
</tr>
<tr>
<td>$P' \rightarrow W'$</td>
<td>$r'$, return of $r'$</td>
<td>$f(r', h(W')) \rightarrow$</td>
</tr>
<tr>
<td></td>
<td>$\leftarrow { r, h(), f() }$</td>
<td>$\leftarrow \text{yes/no}$</td>
</tr>
</tbody>
</table>

(b) Protocol for a token

- Example of a token protocol
### Static Biometric Protocol

#### Example of a static biometric protocol

<table>
<thead>
<tr>
<th>Client</th>
<th>Transmission</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U$, user</td>
<td>$U \rightarrow$</td>
<td>$r$, random number E(), function</td>
</tr>
<tr>
<td>← ${ r, E() }$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$B' \rightarrow BT'$ biometric device $D'$ biometric device $r'$, return of $r$</td>
<td>$E(r', D', BT') \rightarrow E^{-1}E(r', P', BT) = (r', P', BT)$</td>
<td></td>
</tr>
<tr>
<td>← yes/no</td>
<td></td>
<td>if $r' = r$ and $D' = D$ and $BT = BT(U)$ then yes else no</td>
</tr>
</tbody>
</table>

- **user transmits an ID to the host**
- **host responds with a random number and the identifier for an encryption**
- **client system controls biometric device on user side**
- **host decrypts incoming message and compares these to locally stored values**
- **host provides authentication by comparing the incoming device ID to a list of registered devices at the host database**
Dynamic Biometric Protocol

- **host provides a random sequence and a random number as a challenge**
- **sequence challenge is a sequence of numbers, characters, or words**
- **user at client end must then vocalize, type, or write the sequence to generate a biometric signal**
- **the client side encrypts the biometric signal and the random number**
- **host decrypts message and generates a comparison**

### Example of a dynamic biometric protocol

<table>
<thead>
<tr>
<th>Client</th>
<th>Transmission</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U, \text{ user}$</td>
<td>$U \rightarrow$</td>
<td>$r$, random number $x$, random sequence challenge $E()$, function</td>
</tr>
<tr>
<td></td>
<td>$\leftarrow { r, x, E() }$</td>
<td></td>
</tr>
<tr>
<td>$B', x' \rightarrow BS'(x')$</td>
<td>$E(r', BS'(x')) \rightarrow$</td>
<td>$E^{-1}E(r', BS'(x')) = (r', BS'(x'))$ extract $B'$ from $BS'(x')$</td>
</tr>
<tr>
<td>$r'$, return of $r$</td>
<td>$\leftarrow \text{yes/no}$</td>
<td>if $r' = r$ and $x' = x$ and $B' = B(U)$ then yes else no</td>
</tr>
</tbody>
</table>

(d) Protocol for dynamic biometric
## Potential Attacks, Susceptible Authenticators, and Typical Defenses

<table>
<thead>
<tr>
<th>Attacks</th>
<th>Authenticators</th>
<th>Examples</th>
<th>Typical defenses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client attack</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>Guessing, exhaustive search</td>
<td>Large entropy; limited attempts</td>
</tr>
<tr>
<td>Token</td>
<td></td>
<td>Exhaustive search</td>
<td>Large entropy; limited attempts, theft of object requires presence</td>
</tr>
<tr>
<td>Biometric</td>
<td></td>
<td>False match</td>
<td>Large entropy; limited attempts</td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>Plaintext theft, dictionary/exhaustive search</td>
<td>Hashing; large entropy; protection of password database</td>
</tr>
<tr>
<td>Token</td>
<td></td>
<td>Passcode theft</td>
<td>Same as password; 1-time passcode</td>
</tr>
<tr>
<td>Biometric</td>
<td></td>
<td>Template theft</td>
<td>Capture device authentication; challenge response</td>
</tr>
<tr>
<td><strong>Host attack</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>&quot;Shoulder surfing&quot;</td>
<td>User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication</td>
</tr>
<tr>
<td>Token</td>
<td></td>
<td>Theft, counterfeiting hardware</td>
<td>Multifactor authentication; tamper resistant/evident token</td>
</tr>
<tr>
<td>Biometric</td>
<td></td>
<td>Copying (spoofing) biometric</td>
<td>Copy detection at capture device and capture device authentication</td>
</tr>
<tr>
<td><strong>Eavesdropping, theft, and copying</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td>Replay stolen password response</td>
<td>Challenge-response protocol</td>
</tr>
<tr>
<td>Token</td>
<td></td>
<td>Replay stolen passcode response</td>
<td>Challenge-response protocol; 1-time passcode</td>
</tr>
<tr>
<td>Biometric</td>
<td></td>
<td>Replay stolen biometric template response</td>
<td>Copy detection at capture device and capture device authentication via challenge-response protocol</td>
</tr>
<tr>
<td><strong>Replay</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Trojan horse</strong></td>
<td></td>
<td>Installation of rogue client or capture device</td>
<td>Authentication of client or capture device within trusted security perimeter</td>
</tr>
<tr>
<td><strong>Denial of service</strong></td>
<td></td>
<td>Lockout by multiple failed authentications</td>
<td>Multifactor with token</td>
</tr>
</tbody>
</table>
Authentication Security Issues

- **Eavesdropping**: Adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary.
- **Host Attacks**: Directed at the user file at the host where passwords, token passcodes, or biometric templates are stored.
- **Denial-of-Service**: Attempts to disable a user authentication service by flooding the service with numerous authentication attempts.
- **Trojan Horse**: An application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric.
- **Client Attacks**: Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path.
- **Replay**: Adversary repeats a previously captured user response.
Practical Application: Iris Biometric System

Customer domain: personal use device

Customer's PC/laptop
- SecureCam client
- Java
- Browser
- Home banking screens (HTML)
- 20 Kbytes (maximum) compressed iris image file

Internet

Existing IT infrastructure
- Web server
- Firewall
- Local server
- PIN server

Bank intranet

Image + CIN

Status

Bank branch office: public-use device

Enroll or verify station
- Enroll application/GUI
- Link encryption

Bank intranet

Status

Enrollment or verification Iris code + CIN

The existing information technology (IT) structure provides capability for remote transactions. It allows access either by PIN or iris biometric (for higher valued transactions).

The verification server receives an iris code or an iris image that is converted to an iris code. The system matches the iris code and CIN to a database and returns status, allowing or denying access to user's account.

Figure 3.11 Multichannel System Architecture Used to Link Public- and Personal-use Iris Identification Devices via the Internet. The system uses each customer's PIN (personal identification number), iris code, and CIN (customer identification number) to validate transactions. [NEGI00]
Figure 3.12  ATM Architectures. Most small to mid-sized issuers of debit cards contract processors to provide core data processing and electronic funds transfer (EFT) services. The bank’s ATM machine may link directly to the processor or to the bank.
Summary

- Four means of authenticating a user's identity
  - something the individual knows
  - something the individual possesses
  - something the individual is
  - something the individual does

- Vulnerability of passwords
  - offline dictionary attack
  - specific account attack
  - popular password attack
  - password guessing against single user
  - workstation hijacking
  - exploiting user mistakes
  - exploiting multiple password use
  - electronic monitoring

- Hashed password and salt value
- Password file access control

- Password selection strategies
  - user education
  - computer generated passwords
  - reactive password checking
  - proactive password checking

- Bloom filter
- Token based authentication
  - memory cards
  - smart cards

- Biometric authentication
- Remote user authentication
  - password protocol
  - token protocol
  - static biometric protocol
  - dynamic biometric protocol
What’s Next

• Read Chapter 1, 2, and 3
  – Chap 1: Focus on big picture and recurring concepts
  – Chap 2: Identify cryptographic tools and properties
  – Chap 3: How can you authenticate a user?

• Homework  Posted on Course Website
  – Due Tuesday

• Next Lecture Topics from Chapter 4
  – Access Control