Authentication

1. Identity
2. Groups and Roles
3. Network Identities
4. Authentication
5. Biometrics
6. UNIX Authentication

What is Identity?

Computer’s representation of an entity
- Entities can be subjects or objects.
Authentication binds a principal to an identity.

Example:
- *username* expresses your identity.
- *password* binds the person typing to that particular identity (username).
Purpose of Identity

Access Control
- Most systems base access rights on identity of principal executing the process.

Accountability
- Logging and auditing functions.
- Need to track identity across account/role changes (e.g., su, sudo).

Groups and Roles

An "entity" may be a set of entities referred to by a single identifier.

Principals often need to share access to files, and thus are taken as groups.
- **static**: alias for a group of principles.
- **dynamic**: principal changes from one group to another as different privileges are needed.

**role**: a group that ties membership to function

Network Identity

**Ethernet (MAC) Address**
- 48-bit data link level identifier
  - example: 00:0B:DB:78:39:8A

**IP Address**
- 32-bit network level identifier
  - ex: 10.17.0.101

**IPv6 Address**
- 128-bit network level identifier
  - ex: fe80::2a0:c9ff:fe97:153d/64

**Hostname (DNS name)**
- string application level identifier
  - ex: www.nku.edu
What is Authentication?

Binding of an identity to a subject

Based on:
1. What the entity knows (e.g., passwords)
2. What the entity has (e.g., access card)
3. What the entity is (e.g., fingerprints)
4. Where the entity is (e.g., local terminal)

Two-factor authentication

What You Know

- Passwords
- Pass Phrases
- PINs

What You Have

- Smart Cards
- USB Token
- RFID

RFID used for toll collection
USB Tokens and Smart Cards

Small device with storage and processor.
- USB tokens tend to focus on storage.
- Smart cards on processor + small storage.
- Differences are growing smaller.

Methods of use
- By Hand (read card and type one-time password)
- USB
- Wireless

RFID

Radio Frequency Identification

Types of Tags
- Passive: use power from reader signal
- Active: internal power source

Applications
- Product tracking (EPC barcode replacement)
- Transportation payment
- Automotive (embedded in car keys)
- Passports
- Human implants

What You Are: Biometrics

Identification by human characteristics:
1. Physiological
2. Behavioral

A biometric characteristic should be:
1. universal: everyone should have it
2. unique: no two people should share it
3. permanent: it should not change with time
4. quantifiable: it must be practically measurable
How Biometrics Work

1. User submits sample.
2. Software turns sample into digital template.
4. Authentication based on how closely templates match.

Biometric Measurement

Possible Outcomes:

1. Correct person accepted
2. Imposter rejected
3. Correct person rejected (False Rejection)
4. Imposter accepted (False Acceptance)

False Positives and Negatives

Tradeoff between
False Accept Rate
False Reject Rate
Fingerprints

Capacitive measurement, using differences in electrical charges of whorls on finger to detect those parts touching chip and those raised.

Brandon Mayfield

- Fingerprints found in 2004 Madrid bombing.
- Brandon arrested May 6, 2004.
- FBI claimed “100 percent positive” match.
  - Held under a false name.
  - Then transferred to unidentified location.
- Spanish police identify fingerprint as belonging to an Algerian man May 21, 2004.

Eye Biometrics

- Iris Scan
  - Lowest false accept/reject rates of any biometric.
  - Person must hold head still and look into camera.
- Retinal Scan
  - Cataracts and pregnancy change retina pattern.
  - Lower false accept/reject rates than fingerprints.
  - Intrusive and slow.
Other Types of Biometrics

<table>
<thead>
<tr>
<th>Physiological</th>
<th>Behavioral</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA</td>
<td>Gait recognition</td>
</tr>
<tr>
<td>Face recognition</td>
<td>Keyboard dynamics</td>
</tr>
<tr>
<td>Hand geometric</td>
<td>Mouse dynamics</td>
</tr>
<tr>
<td>Scent detection</td>
<td>Signatures</td>
</tr>
<tr>
<td>Voice recognition</td>
<td></td>
</tr>
</tbody>
</table>

Biometrics are not infallible

What are False Accept and Reject Rates?
Do the characteristics change over time?
- Retina changes during pregnancy.
- Fingerprint damage due to work/pipesmoking.
- Young and old people have fainter fingerprints.

Is it accurate in the installed environment?
- Is someone observing fingerprint or voiceprint checks?
- i.e., did you collect biometric from the person?

Biometrics can be compromised.

Unique identifiers, not secrets.
- You can change a password.
- You can't change your iris scan.

Examples:
- You leave your fingerprints every place.
- It's easy to take a picture of your face.

Other compromises.
- Use faux ATM-style devices to collect biometrics.
- Obtain all biometric templates from server.
Use and Misuse of Biometrics

Employee identification.
- Employee enters login name.
- System uses fingerprint to verify employee is who he claims to be.
- Problem: Does biometric match the employee?

Criminal search (Superbowl 2001)
- System uses face recognition to search for criminals in public places.
- Problem: Does any biometric in database match anyone in a crowd of people?
- Assume system is 99.99% accurate and 1 in 10 million people is a terrorist. Result: 1000 false positives for each terrorist.

Location

Classic: only allow access from a particular terminal or a particular set of remote hosts.

Modern: GPS-based
- Location Signature Sensor (LSS) for host and user.
- Access rules permit user only to access host with specific LSS values.
- Cell-phones track location, and some states use them to track drivers' speed and locations.

UNIX Authentication

UNIX identifies user with a UID
- Username is for humans, UID for computers.
- 15-bit to 32-bit unsigned integer.
- UID=0 is the superuser, root.

Identity and authentication data stored in
- /etc/passwd
- /etc/shadow
- /etc/group
/etc/\{\texttt{passwd, shadow}\}

Central file(s) describing UNIX user accounts.

\texttt{/etc/passwd}
- Username
- UID
- Default GID
- GCOS
- Home directory
- Login shell

\texttt{/etc/shadow}
- Username
- Encrypted password
- Date of last pw change.
- Days 'til change allowed.
- Days 'til change required.
- Expiration warning time.
- Expiration date.

student:x:1000:1000:Example User,,555-1212,:/home/student:/bin/bash
student$:1$w/UuKtLF$otSSvXtSN/xJeUOGFENztb13226:0:99999-?:::

Groups and GIDs

GIDs are 32-bit non-negative integers. Each user has a default GID.
- File group ownership set to default GID.
- Temporarily change default GID: \texttt{newgrp}.

Groups are described in \texttt{/etc/group}
- Users may belong to multiple groups.
- Format: group name, pw, GID, user list.
  - wheel:x:10:root,waldenj,bergs

Superuser Powers

Superuser can
- Read any file.
- Modify any file.
- Add / remove users.
- Become any user.
- Kill any process.
- Reprioritize processes.
- Configure network.
- Set date/time.
- Shutdown / reboot.

Superuser can’t
- Change read-only filesystem.
- Decrypt hashed passwords.
- Modify NFS-mounted filesystems.
- Read or modify SELinux protected files.
Switching Users

The `su` command allows you to switch users.

```
$ id
uid=102(wj) gid=102(wj) groups=102(wj)
$ su
Password:
# id
uid=0(root) gid=0(root)
groups=0(root),1(bin),2(daemon),3(sys),4(adm),
6(disk),10(wheel)
# su john
john$ id
uid=1995(john) gid=1995(john) groups=1995(john)
john$ exit
# exit
$ id
uid=102(wj) gid=102(wj) groups=102(wj)
```

Real and Effective UIDs

**Real UID**
- The UID matching the username you logged in as.

**Effective UID**
- The UID that is checked for access control.
- The `su` command changes your EUID.

**SUID programs**
- A SUID program executes with an EUID of the owner of the program instead of yours.
- `/usr/bin/passwd` is SUID root. Why?

Key Points

1. Access control is based on identity.
2. Authentication consists of an entity, the user, attempting to convince another entity, the verifier, of the user’s identity
   1. something you know
   2. something you have
   3. something you are
3. Authentication Types
   1. Passwords
   2. Security Tokens
   3. Biometrics
References