Topic 7

Authentication Overview

We take on user authentication from a network-based viewpoint.  
A network's first line of defense is user authentication.  
Its goal is to stop unauthorized users from accessing a network.  
It is the basis of how access controls are set.  
It serves to hold users accountable.

**Verifying user identity**

User authentication has two steps:

Identification: introducing the user to the security system.

Verification: supplying data that connects the object and the identification.

The process through which a user claims their identity is known as identification.

The method used for verifying such claim is verification.

**2 passwords**

Most common means of authentication.

Require no special hardware

Common password-based authentication

The user enters their password and username.

The relevant database table is searched by the system for the username.

Verifies the existence of the username and password pair

allows the user to access the system

**Password strength**

If allowed, users frequently choose weak passwords.

Simple to break through dictionary attack

It's possible to make users produce more complicated passwords.

Users can obtain a strong password from the system.

A stronger password may be written down by many users, which provides a bigger security risk than a weak password.

**Attacks on password security**

An attacker might be able to "listen" in and obtain password information by eavesdropping.

The password database can be directly attacked in order to find or change passwords.

Sessions can be taken over by an attacker who disconnects the target while staying online.

Never use the same password across different applications.

**Losing Passwords**

It is usual for users to lose or forget their passwords.

can be resolved by often changing passwords.

Using password generators is one way to update your password.

create new passwords automatically by using a master secret.

**Cracking Hashed passwords**

Hashing works on the principle that it would be very hard to crack a hashed password through trial and error.

This isn't the case if people use short, easy passwords.

To maintain a high level of security, strong passwords are still necessary for the hashing function.

**Multi-Factor Authentication**

Multiple verification techniques are used to authenticate and verify an identity.

Signal factor authentication is user/password authentication.

* just one means of verification—the password.

A more robust method of confirmation.

used in situations where security is a top priority.

* An ATM card with PIN, for instance

**Disadvantage**

Cost

* Cost of supplying smartcards, USB tokens, etc.
* Cost of hardware/software to read the tokens

Inconvenience

* Users may not like inconvenience of having to carry around a token.

The sensitivity of the data and transactions that are protected must be balanced with the cost and inconvenience of security.

**Increased Security-Probability**

The likelihood that the right verification information will be generated at random is significantly reduced when two or more verification techniques are combined.

Voiceprint

There is around a 1 in 10000 chance of matching.

PIN

There is a 1 in 10000 chance of guessing a PIN.

Combined

There is a 1 in 100000000 chance of matching both

**Registering Biometric Data**

The biometric system is registered by the user.

Biometric data measurements are made.

Able to collect many biometric data readings if necessary.

To create a template, the measurement is subjected to an algorithm.

A database stores the template.

**Authenticating Biometric Data**

User provides the system with their identity. (e.g., username).

A measurement of the user's biometric data is obtained.

Again, converted into a digital template.

This template compares with the database template.

Look for any matches.

The matching process is approximate.

The user gets authenticated if their biometric data matches the template that has been stored.

**Matching Biometric Data**

Not an exact science.

* Biometric data measurements never really match up.

When a user first registers in the system, several measures are made.

A successful match is one that matches the template.

The algorithm that matches the templates has tolerances in it.

**Fingerprints**

Fingertip ridges and valleys are specific to each individual fingertip.

* Long-used by police

most popular biometric technique

accessible for PCs and laptops

System accessibility made possible via touch technology

**Face Recognition**

Take a picture of your face in the viewable range.

* Use a standard camera
* Use central portion of face
* Extract features that remain constant over time.

Avoid changing features, e.g., hair

An alternate version shows an image of a face's heat emission in infra-red.

Most users accept to using these systems.

Issues brought on by masks, lighting, etc.

**Speech Recognition**

Individuals' speech differs in certain aspects.

The speaker's anatomy is reflected in these patterns.

These patterns reflect the patterns of speech learned as a result of:

• Location

• Peers

• Language

**Iris Recognition**

Iris is the colored area around the pupil.

It is believed that iris patterns are distinct.

An image of the iris is captured by video systems.

Becoming more financially feasible as the cost of equipment has decreased.

Functions with both contact lenses and glasses.

**Hand Geometry**

Can utilize measures of fingers or whole hands

Length, Width, Thickness, Surface area

Used for access control in commercial and residential premises

**Written Signatures**

Uses measurement of the way the signature is written not just the final signature

Can measure a range of parameters:

• Speed

• Pressure

• Angle of writing

Used in business applications where a signature is commonly used to identify a user

**Errors in Biometric Systems**

possesses a false accept rate (FAR), which measures how quickly the system accepts an invalid user.

possesses a false rejection rate (FRR), which measures the frequency at which the system rejects an authorized user.

By modifying certain factors, it is feasible to modify both rates in numerous systems.

Modern systems have low rates for both.

**The Market Leader**

The usage of fingerprint authentication is common.

Many laptops and computer accessories have fingerprint readers integrated into them.

They are reasonably priced.

Permit user to authenticate by placing finger on reader.

Can be used for two-factor authentication with password or PIN.