جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم
قسم الأمن السيبراني

Lecture: (2)

Human Authentication

Subject: authorization and access control
second Stage
Lecturer: Asst. Lecturer. Suha Alhussieny

Authentication can be divided into two major categories.

1. **Human to machine authentication**
2. **Machine to machine authentication**

In any of the above types of authentication, there is a requirement for certain credentials. In human verification, we have a user ID and password set by the consumer, while for machines, we have certificates and IP addresses, along with other information.

Generally, a consumer has to select or create a User ID and corresponding password for that unique ID that the system will use to verify user credibility. Many companies make use of authentication to verify the users who try to login into their digital platforms. But if consumers' data falls into cybercriminals' hands, it can cause some severe problems. Hence companies ensure using high-level security measures, which involves using another advanced authentication level such as multi-factor authentication.

Human authentication

Human authentication, in the context of information security, is the practice of assessing a human's credentials before allowing them access to a protected system or data. The accessibility, confidentiality, and secrecy of data and resources may be protected through this procedure by limiting access to only people have been granted permission to use them. The combination of multiple biometric features captured by image sensors to improve the efficacy and dependability of human authentication and recognition systems.

IDENTIT

Question: How do you identify people?

identity is the unique set of characteristics that can be used to identify a person as them self and no one else.

The word can be used in different ways in different contexts.

On a personal level, *identity* often refers to a person's sense of self, meaning how they view them self as compared to other people.

Practically speaking, a person's *identity* is who they really are.

• Digital identity: data that describes a person and its relationship to others

• A person could have many digital identities, some overlapping, some contradictory

• Data could be incorrect, outdated, incomplete

Aspects of digital identity:

Name, NetID, Email address, URL, IP address, Citizenship, Political party

Attribute: property of a principal

• name is "Cecil Sagehen", birthdate is 11/29/1913

• Identity: set of attributes

• each principal may have many identities of use in different

scenarios (student, taxpayer, athlete)

• Identifier: an attribute that is unique within a population

• Verifier: an attribute that is hard to produce hence can be

used as a basis for authentication

Enrollment

• Enrollment: establishing identity with a system

• Create an account

• Get an ID card, visa

• Register a machine on a network

• Get a signing key from a provider

• System might (not) verify claimed attributes during enrollment

• Websites rarely do

• Governments often do

What is an authentication factor?

An authentication factor is a special category of security credential that is used to verify the identity and authorization of a user attempting to gain access, send communications, or request data from a secured network, system or application.

What is the difference between authentication and authorization?

Authentication and authorization may sound similar, but they explain two completely different functions. It's important to distinguish between these two concepts and the role they play in protecting data and other valuable information from unauthorized access.

- *Authentication* is the act of proving the identity of an individual **(Are you who you say you are?).**
- *Authorization* is about proving the access rights of that individual**(Are you allowed to do that?).**

So even if a person successfully verifies their identity, it's not certain that they have the authorization to access certain systems or information. In that way, authentication and authorization both play a crucial role in digital security.

5 Types of Authentication Factors

Understanding the diverse landscape of authentication factors is the foundation of building a robust security system. The five key types of factors: Knowledge-Based, Possession-Based, Inherence-Based, Location-Based, and Behavior-Based, offer various ways to confirm a user's identity.

Whether you're tasked with safeguarding a digital system or limiting physical access to a facility, grasping the nuances of these five factors will empower you to make informed decisions. Here's a closer look at each:

1) Something You Know (Knowledge-Based)

Knowledge-based factors are the foundation of most authentication systems. They represent the information only you should know.

- **Passwords**: The most common form of a knowledge factor. However, strong passwords should be unique, complex, and never reused across different platforms.

- **Security Questions**: Used as a backup authentication method for password recovery, security questions can sometimes serve as a second knowledge factor.
- **Personal Identification Number (PIN)**: Often used in conjunction with other authentication methods, such as smart cards, to add an extra layer of security.

While knowledge factors are easy to implement, they are vulnerable to various forms of attacks, including phishing and social engineering. Thus, they are often combined with other factors in multi-factor authentication systems for enhanced security.

2) Something You Have (Possession-Based)

Possession-based factors validate a user's identity by requiring a physical object that only the legitimate user should have, adding another layer to the authentication process.

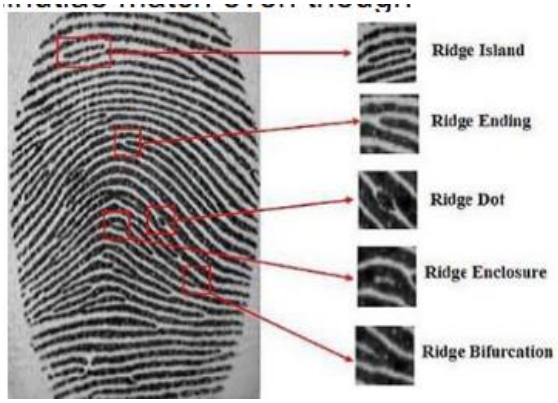
- **Smart Cards**: Widely used in corporate settings, smart cards are physical cards that contain user information.
- **Security Tokens:** These are hardware devices that generate one-time passwords for login.
- **One-Time Passwords (OTP):** These are temporarily valid codes generated by apps or physical devices.

These are just a few examples. Possession factors add complexity to the authentication process, making it more challenging for unauthorized users to gain access. However, while these factors enhance security, they can still be vulnerable, especially if the possession item is lost or stolen.

3) Something You Are (Inherence-Based)

In modern-day authentication, inherence-based factors, which are also referred to as biometrics, are increasingly gaining popularity. These factors are derived from your distinctive physiological traits, and are rapidly becoming the preferred choice for authentication due to their potent combination of robust security and user convenience.

- **Fingerprint Scans**: Widely used in smartphones and secure facilities, fingerprint scans offer a quick yet secure means of authentication.



- **Facial Images**: Facial recognition is increasingly common, especially in mobile devices and restricted-access buildings.