



جامعة المستقبل
AL MUSTAQBAL UNIVERSITY



قسم الامانة
السيبرانية
DEPARTMENT OF CYBER SECURITY

SUBJECT:

AUTHENTICATION AND ACCESS CONTROL

CLASS:

SECOND

LECTURER:

DR. SUHA ALHUSSIENY

LECTURE: (2)

HUMAN AUTHENTICATION



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- Data could be incorrect, outdated, incomplete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.

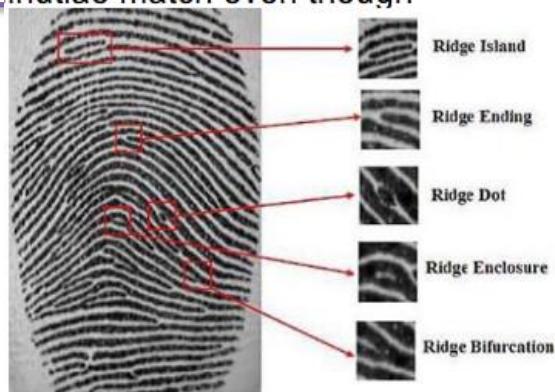
- **Smart Cards:** Widely used in corporate settings, smart cards are physical cards that contain user information.
- **Security Tokens:** These are hardware devices that generate one-time passwords for login.
- **One-Time Passwords (OTP):** These are temporarily valid codes generated by apps or physical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

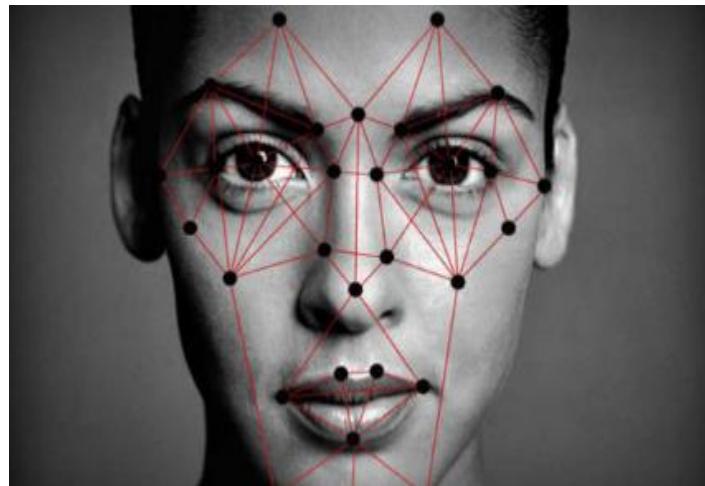
3) Something You Are (Inherence-Based)

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.



- **Iris Scans:** Known for high accuracy, [iris scans](#) are used in more stringent security settings.

Biometric authentication offers a unique blend of security and user-friendliness, making these inheritance-based factors an increasingly popular choice in multi-factor authentication methods.

4) Somewhere You Are (Location-Based)

Location-based factors take into account the geographical location of the user attempting to gain access, offering a unique angle to authentication.



- **Geo-Fencing:** Grants access only when the user is in a specific geographical area.
- **IP Address Verification:** Allows access only from certain IP addresses, often used in corporate settings.

Location-based factors are generally supplemental but can provide an added layer of security for specific applications such as network access restrictions, remote work verification, and enhanced mobile banking security.

5) Something You Do (Behavior-Based)

These are relatively new and less common but are growing in popularity due to their ability to continuously authenticate users based on behavior.

- **Keystroke Dynamics:** Studies the unique way a user types on a keyboard.
- **Mouse Movement Patterns:** Analyzes the way a user moves the mouse while interacting with a system.

Behavior-based factors are still evolving but hold great promise in the context of multi-factor authentication, especially when combined with biometric systems and other traditional factors.

Understanding these five key authentication factors offers a comprehensive view into the choices available for securing both digital and physical environments. In the following section, we'll dive into practical considerations for choosing the right combination of these factors to meet your specific security needs.

How to Choose Authentication Factors for Your Needs

1) Assess the Risk Profile



It's essential to understand the risk level associated with what you are protecting, be it a data center or a restricted area within a facility.

- **High-Security Scenarios:** In settings where extremely sensitive data or valuable assets are involved, such as bank vaults or secure data centers, multi-factor authentication (MFA) using at least two different categories of authentication factors is advisable.
- **Moderate-Risk Scenarios:** A strong primary factor, like a biometric scan, could be complemented with a secondary factor, such as a smart card, for added assurance.
- **Low-Risk Scenarios:** A newsletter subscription page online or an employee lounge might just require a username and password, or a simple employee badge, for access.

2) User Experience and Convenience

Regardless of the environment, the ease with which users can authenticate themselves is critical to system compliance and overall satisfaction.

- **Ease of Use:** Consider factors that the user can easily manage. For instance, consider systems like facial recognition or quick and unobtrusive access in high-traffic areas like the main entrance of an office building. These provide a faster, more convenient experience than, say, a complex password or fumbling for an access card. at a turnstile.
- **Accessibility:** Ensure that your chosen factors are inclusive and accessible to all users, including those with disabilities. For instance, RFID badges can be more convenient for those who may struggle with biometric scans due to physical disabilities.



3) Implementation Costs and Complexity

The costs, both financial and in terms of complexity, can vary widely based on your choice of authentication factors.

- **Budget Considerations:** Selecting a security measure involves balancing safety and budget. While passwords and security questions are cheap, they lack robust protection. High-end biometric systems are expensive upfront but provide higher security ROI in the long run. Careful consideration of facts and details can help achieve a balance between security and budget.
- **Maintenance:** Don't forget to account for the ongoing expenses related to software updates, as well as maintenance or replacement of physical components like biometric scanners or security key fobs.

4) Versatility and Adaptability

The factors you choose should be versatile enough to handle various situations and scalable to meet future requirements.

- **Scalability:** An authentication system should be able to adapt to growing needs, whether that means adding new access points in a building or accommodating a growing online user base.
- **Interoperability:** Your chosen methods should integrate smoothly with your existing digital systems or physical security infrastructure, making future upgrades less complicated.

5) Compliance and Regulatory Requirements

Compliance isn't just a box to tick; it's an ongoing responsibility that has both legal and financial implications.



- **Data Protection Laws:** For digital platforms, this could mean GDPR compliance, while physical security may involve adhering to building codes and safety standards.
- **Industry-Specific Regulations:** Different sectors have their own sets of guidelines. For example, financial and healthcare institutions often need to meet stringent regulations such as PCI DSS or HIPAA that might necessitate multiple authentication factors.

Choosing the right authentication factors isn't just a question of selecting the most advanced technologies available. It's about finding a tailored solution that fits your specific needs and constraints. The ideal choice often involves a mix of factors, sometimes even from the same category, to create a robust multi-factor authentication system that balances user convenience with high-level security. So, whether you are managing access to a secured network or a mobile app, keep these practical considerations at the forefront of your decision-making process.

Is it possible to achieve human authentication without compromising privacy?

Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.

The short answer is yes. Let's assume for a moment that Musk is calling for the use of biometrics in the authentication process (tying people to identities). People would still be able to use an alias as an identity; biometrics would simply be the way that identity was verified. In this way, privacy on Twitter through the use of aliases would be maintained.



But even for people who don't use aliases, there may be some privacy concerns around Twitter collecting and holding their sensitive biometric data. What if this huge database were to be compromised? The good news is there are storage techniques available that can help prevent this — for instance, storing identification data separately from biometric data. In this case, even if a hacker were able to access the biometric data without the accompanying identification details, it would be rendered completely useless.

H.W/

- 1.** Authentication can be divided into:
- 2.** Which credentials are typically required for human verification?
- 3.** Human authentication ensures:
- 4.** Identity refers to:
- 5.** A digital identity can include:
- 6.** Which of the following describes an identifier?
- 7.** Which of the following is a verifier attribute?
- 8.** The process of establishing identity with a system is called:
- 9.** Which statement correctly describes authentication vs. authorization?
- 10.** Which is NOT one of the five types of authentication factors?
- 11.** Passwords, PINs, and security questions are examples of:
- 12.** Smart cards, tokens, and OTPs are examples of:
- 13.** Fingerprints, facial images, and iris scans are examples of:
- 14.** Which is an example of a location-based factor?
- 15.** Keystroke dynamics and mouse movement patterns are examples of:
- 16.** High-security scenarios usually require:
- 17.** Which factor is important for user convenience and compliance?
- 18.** Implementation cost considerations include:



- 19.** Scalability and interoperability are part of:
- 20.** Which method can achieve human authentication without fully compromising