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

- **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 inherence-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.