
Authentication

Introduction to Authentication

Definition of Authentication: The process of verifying the identity of a user, system, or device to grant access.

Significance: Critical in preventing unauthorized access and protecting sensitive information.

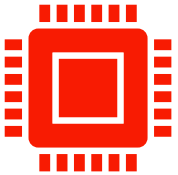
Importance of Authentication

Protecting Confidential Information: Safeguarding sensitive data from unauthorized access.

Compliance: Meeting regulatory requirements and industry standards.

Building Trust: Establishing trust between users and systems.

Authentication Factors



Knowledge-Based Factors: Something the user knows (e.g., passwords, PINs).

Possession-Based Factors: Something the user has (e.g., security tokens, smart cards).

Inherence-Based Factors: Something the user is (e.g., biometrics like fingerprints, facial recognition).

Common Authentication Methods

Password Authentication: Still widely used but susceptible to vulnerabilities.

Two-Factor Authentication (2FA): Adding an extra layer of security with a second authentication factor.

One-Time Passwords (OTP): Temporary codes for a single login session.

Multi-Factor Authentication (MFA)

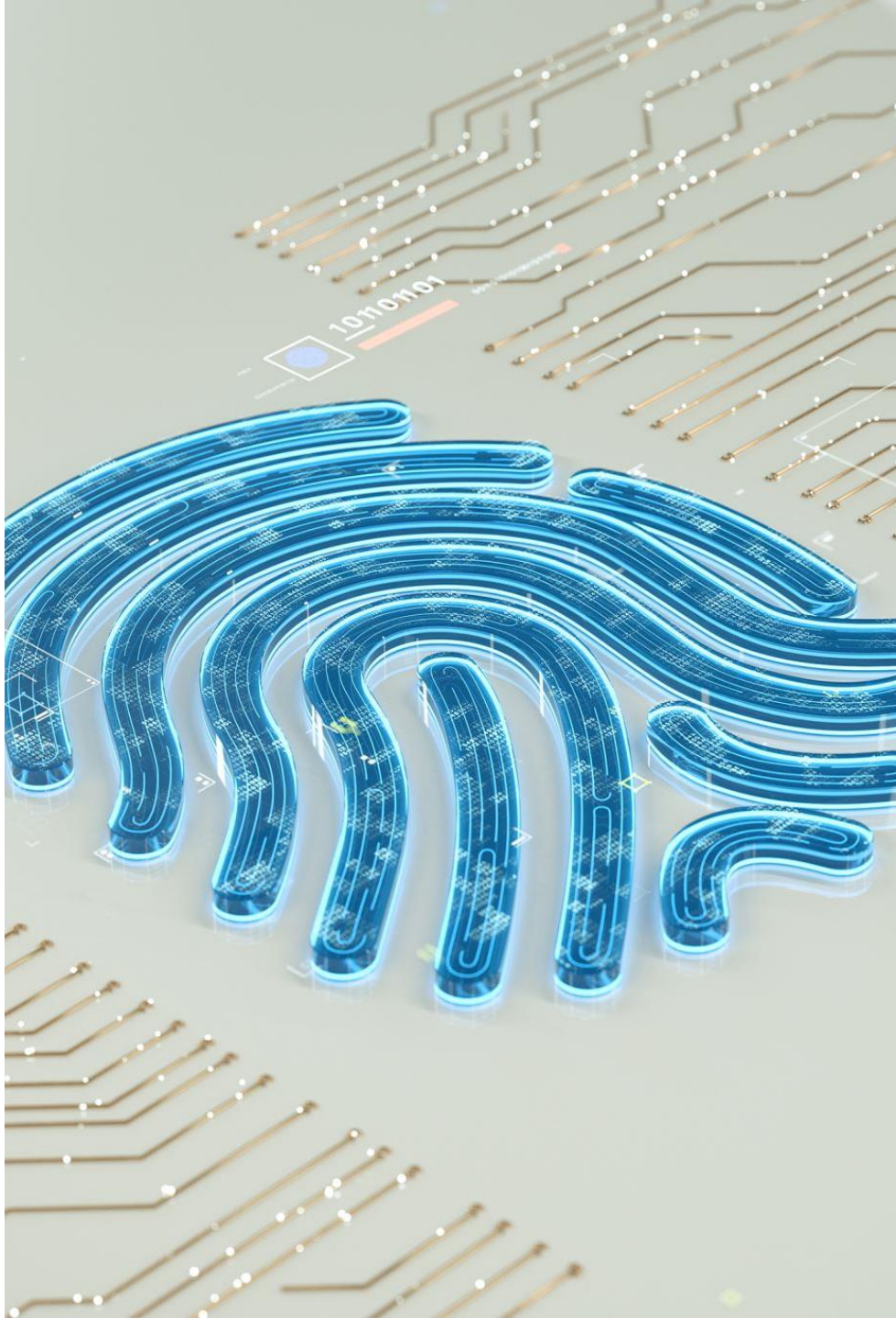
- Definition: Authentication using two or more factors from different categories.
- Enhancing Security: Providing an additional layer of protection against unauthorized access.
- Examples: Using a combination of passwords, security tokens, and biometrics.

Biometric Authentication

Definition: Using unique biological traits for identity verification.

Types: Fingerprint recognition, facial recognition, iris scans, voice recognition.

Advantages and Challenges: Discuss the strengths and potential concerns of biometric authentication.



Security Considerations

Password Policies: Implementing strong password requirements.

Account Lockout Policies: Preventing brute-force attacks.

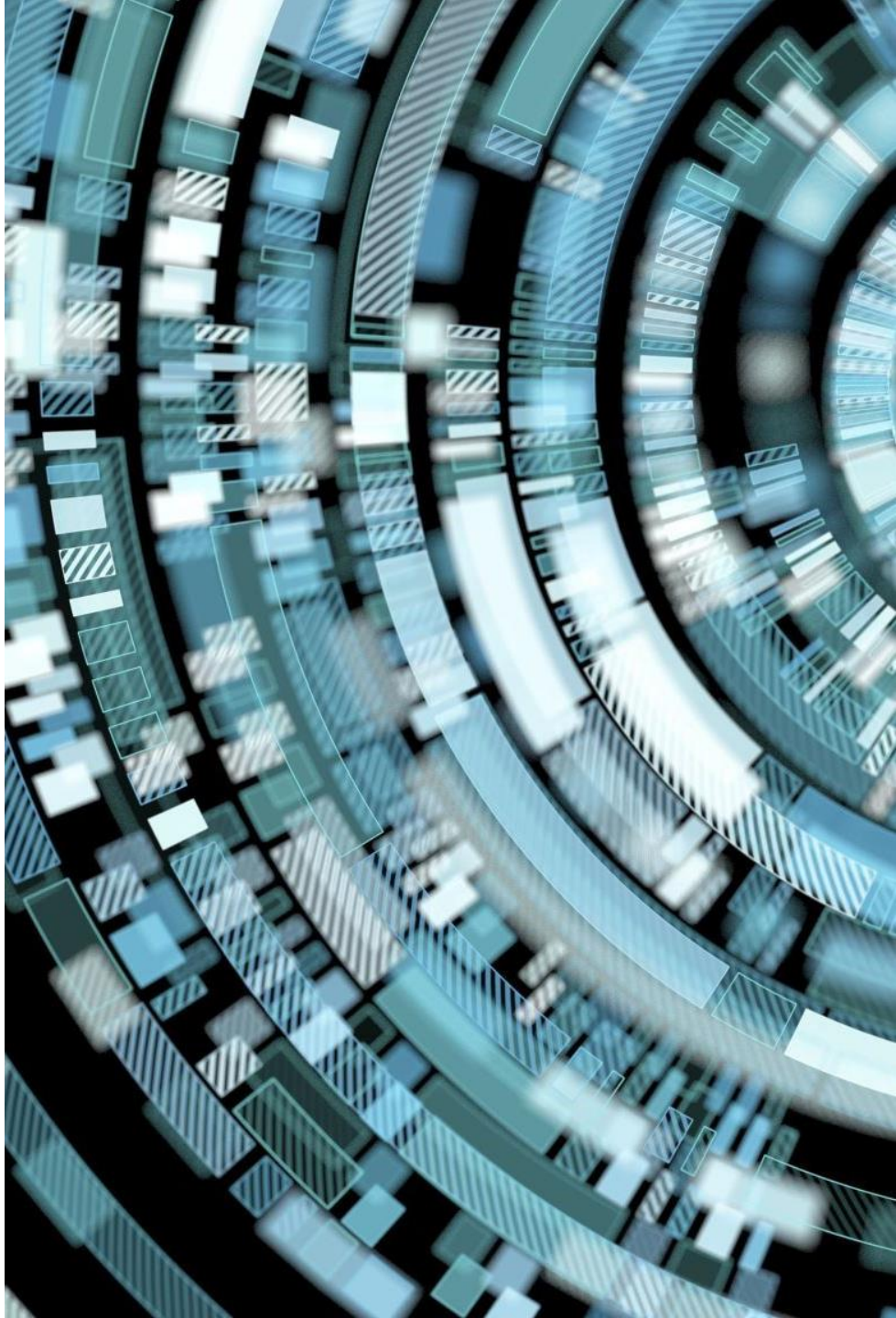
Continuous Monitoring: Monitoring user activities for unusual behavior.

Future Trends

Passwordless Authentication: Moving away from traditional passwords.

Behavioral Biometrics: Analyzing user behavior for authentication.

Artificial Intelligence (AI) in Authentication: Enhancing security through AI-driven solutions.



IBM Z MFA 2.2 supports many authentication factors and implementations:

- Support for pluggable authentication modules (PAMs), that run on Linux
- Support for RSA SecurID authentication
- Web-based password reset function when able to authenticate to MFA policies

Resource Access Control Facility (RACF)

- IBM offers RACF to manage user access control to critical resources with ease
- RACF can log attempts to access unauthorized resources, allowing for active cyber defense