Authentication and Access Control: Securing Digital Access

Authentication vs. Authorization: A Clear Distinction

Authentication: Verifying Identity

Authentication is the critical process of confirming a user's identity. It's about proving you are who you claim to be. Whether it's a password, fingerprint, or security token, this step prevents impersonation, safeguarding sensitive data across all digital systems.

- Confirms "It's me, not someone else."
- Essential for banking, cloud, and government portals.

Authorization: Defining Permissions

Once authenticated, authorization dictates what actions a verified user can perform. It answers the question: "What can this user do?" This includes permissions such as deleting files, editing data, or accessing confidential information.

- Determines user capabilities and access levels.
- Governs actions post-identity verification.

The Perils of Password-Based Authentication

Passwords, though traditional, pose significant risks due to human behaviour and common vulnerabilities:

- Weak password choices (e.g., "123456").
- Password reuse across multiple systems.
- Sharing or writing down passwords.

To mitigate these, **strong password policies** are crucial:

- Minimum 12 characters (16+ recommended).
- Mix of uppercase, lowercase, digits, and special characters.
- Avoid personal information or common words.
- No reuse of previous passwords.
- Regular updates (every 90 days).

One-Time Passwords (OTPs): Enhanced Security

One-Time Passwords (OTPs) offer a significant leap in security by being valid for a single use only. Once used or expired (typically within 30 seconds), an OTP cannot be reused. This mechanism thwarts attackers who might intercept a password, as its validity window is too brief for exploitation.

How OTPs Function

Both the server and the user's device (e.g., smartphone, USB generator) employ synchronised algorithms. The device generates an OTP, which the user then inputs into the system. The server verifies this against its own calculation, granting access if a match is found within the valid timeframe.

Delivery Methods:

SMS: Simple, but vulnerable to interception.

Authenticator Apps (e.g., Google Authenticator): More reliable and secure.

Physical Token Generators: The most robust option.

Email: Convenient, but also susceptible to compromise.

Advantages and Disadvantages

Advantage: Even if your primary password is compromised, an attacker cannot gain access without the unique OTP.

Disadvantage: Losing your device (e.g., smartphone, generator) means losing access. Hence, OTPs are frequently integrated into multi-factor authentication (MFA) alongside a master password.

Hardware Tokens and Smart Cards: Tangible Security

Physical Device Requirement

These methods necessitate a physical device for authentication, such as a USB token or a smart card. This physical presence makes unauthorised access extremely difficult, as information cannot be easily stolen without the device itself.

Smart Card Technology

Smart cards feature an integrated circuit and processor, securely storing a private key, public key certificate, and data. When a PIN is entered, the card internally signs data, preventing the key from being transmitted and intercepted. This makes forgery exceptionally challenging.

Real-world Applications:

Government Institutions (e.g., Kazakhstan): Utilise smart cards for Electronic Digital Signatures (EDS).

Commercial Banks: Employ tokens for 2FA in online banking.

Large Corporations: Distribute USB tokens for secure corporate system logins.

Considerations:

- Physical possession required; risk of loss.
- Requires a reader for computer connection.
- More complex administration.

Biometric Authentication: You Are The Key

Biometric authentication represents the cutting edge of security, leveraging unique biological characteristics to verify identity. It transforms the user into the authentication key.

Fingerprints

Each fingerprint is unique, even among identical twins. Systems scan fingers, extract distinct features (minutiae, branch points), and store them as a reference. Subsequent scans are compared for authentication.

Iris Recognition

The human iris boasts 266 independent characteristics, making it incredibly unique. Infrared light scans and analyses the iris structure for highly secure identification.

Face Recognition

This technology analyses distances between key facial feature points (e.g., eye-to-nose distance, cheek shape). Advanced systems like Apple Face ID also incorporate skin texture scanning for enhanced accuracy.

Voice Analysis

Voice authentication analyses the frequency spectrum, timbre, and rhythm of an individual's speech, providing another unique biometric identifier.

Advantages and Disadvantages

Advantages:

- Impossible to lose (it's part of you).
- No passwords to remember.
- Difficult to fake.

Disadvantages:

- Irreversible if biometric data is compromised (e.g., stolen fingerprint).
- Rarely used as the sole authentication factor; typically part of multi-factor systems.

Multi-Factor Authentication (MFA): Layers of Defence

Multi-Factor Authentication (MFA) fortifies security by requiring two or more independent verification methods. This ensures that even if one factor is compromised, access remains secure.

1

Two-Factor Authentication (2FA)

Requires two distinct methods of identity verification. For example, a password combined with an SMS code, or a password and a physical smart card. This prevents unauthorised access even if one factor is stolen.

2

Multi-Factor Authentication (MFA)

Involves three or more authentication factors, such as a password, fingerprint, SMS code, and time-based code. This provides an even more robust security posture.

Authentication Factors Categorised

1

What You Know

Passwords, PINs, security questions.

2

What You Have

Tokens, smart cards, smartphones.

3

What You Are

Fingerprints, iris scans, face, voice.

4

Where You Are

Geolocation (IP, GPS).

5

When You Enter

Login time (detecting unusual activity).

6

How You Behave

Typing speed, phone angle, mouse movements.

Adaptive Authentication: This intelligent system assesses risk dynamically. If logging in from an unfamiliar device, location, or at an unusual time, it requests additional factors. For routine logins, checks may be streamlined for user convenience.

Access Control and Rights Management

Once a user's identity is verified through authentication, the next crucial step is **authorization**: determining precisely what actions that user is permitted to perform within the system.

Key Access Control Models

Role-Based Access Control (RBAC)

Users are assigned specific roles (e.g., Administrator, Manager, Operator), and each role has predefined permissions. This simplifies management by granting rights based on job function.

Attribute-Based Access Control (ABAC)

Permissions are granted dynamically based on a combination of attributes associated with the user, the resource, and the environment. This offers highly granular and flexible access control.

RBAC in Practice

When a user logs in, the system retrieves their assigned role and corresponding rights. For instance, "Ivan Petrov, role 'manager_sales_sales'" would be granted all the permissions of a sales manager.

Linux: The `chmod 755` command dictates file permissions (read, write, execute) for owner, group, and others.

Windows: Access Control Lists (ACLs) define specific permissions for folders or files, often linked to user groups (e.g., "Accounting group only").

Active Directory: Users added to groups like 'IT_Support' automatically inherit administrator rights for their workstations.

Practical Principles of Access Control

1

Principle of Least Privilege

Grant users only the minimum rights necessary to perform their tasks. An accountant should not access programming source code, and a programmer should not alter employee salaries.

2

Access Revocation

Crucial for security: immediately disable accounts for departing employees across all systems. Delays can expose confidential data to former staff.

3

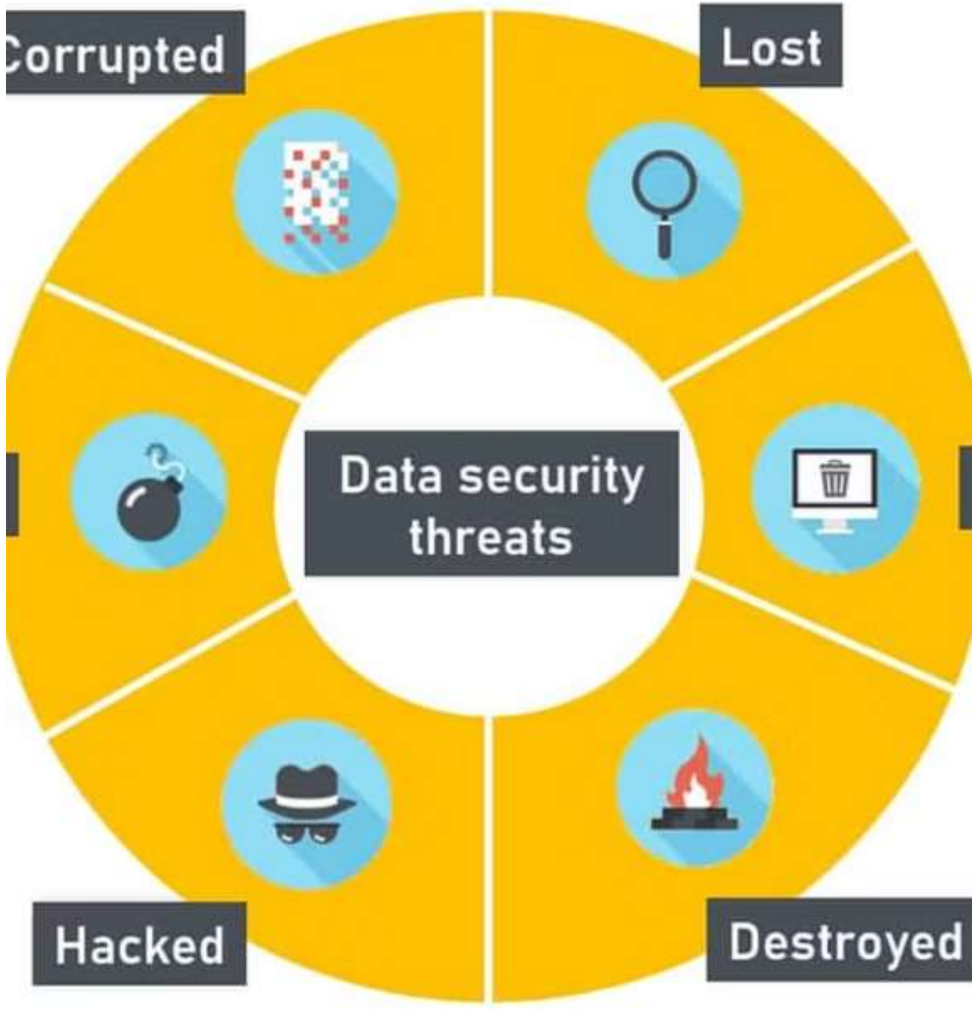
Comprehensive Logging

Maintain detailed logs of all user actions (who, when, what). In the event of an incident (e.g., data theft), this allows for a precise forensic investigation.

4

Periodic Audits

Regularly review and update user rights and permissions. Monthly checks ensure that access privileges remain appropriate and current.



Typical Authentication Attacks and Defences

1

Phishing

Attackers create fake websites or messages to trick users into revealing credentials. **Defence:** 2FA, vigilance with browser URLs, SSL certificate verification, and user training.

2

Brute Force

Programs systematically attempt all possible password combinations. **Defence:** Account lockout policies (e.g., after 5 failed attempts), complex passwords (12+ characters), and 2FA.

3

Man-in-the-Middle (MITM)

Attackers intercept communication between a user and server to steal data. **Defence:** HTTPS encryption, 2FA, VPNs, and verified certificates.

4

Social Engineering

Attackers manipulate individuals into divulging confidential information (e.g., impersonating IT support). **Defence:** Employee training, strict "no password sharing" policies, and identity verification protocols.

Security Questions

- Define authentication and authorisation, highlighting their differences with examples.
- Why is a single password insufficient for modern security? What are its inherent problems?
- Explain the mechanism of One-Time Passwords (OTP) and their superiority over regular passwords.
- What constitutes two-factor authentication? Provide three real-world examples.
- Compare biometric authentication with traditional passwords, outlining advantages and disadvantages.
- How does Role-Based Access Control (RBAC) function? Illustrate with an example from Windows or Linux.
- Name four common authentication system attacks and their respective defence mechanisms.

List of References

- GOST R ISO / IEC 27001: 2013. Information technologies. Information security management.
- GOST R 34.10-2001. Information technology. Cryptographic protection of information.
- Moldovyan A. A., Moldovyan N. A., Sovetov B. Ya. Cryptography: a textbook. St. Petersburg: LanPubl., 2000.
- Partyka T. L., Popov I. I. Informatsionnaya bezopasnost': uchebnoe posobie [Information Security: a textbook]. Moscow: FORUM-INFRA-M, 2002.
- Management of identification and authentication in networks, Moscow: DMK-Press, 2008.
- Galatenko V. A. Fundamentals of information security. Course of lectures, Moscow: INTUIT Publ., 2008.
- NIST SP 800-63-3. Digital Identity Guidelines. US Government, 2017.