UDC 004

Karyna Polishchuk, Master's Student,
Oleksii Chyzhmotria, Senior Lecturer
Zhytomyr Polytechnic State University

SYSTEMATIZATION AND CLASSIFICATION OF MULTIFACTOR AUTHENTICATION METHODS

The increasing number of cyber threats and the growing complexity of digital ecosystems have led to the widespread adoption of multifactor authentication (MFA) as a key mechanism for strengthening information security. However, the diversity of MFA implementations across platforms and technologies necessitates the development of a clear and unified classification system. The systematization of MFA methods enables a better understanding of their structure, security characteristics, and practical applicability within different organizational environments.

Traditionally, MFA mechanisms are categorized according to the authentication factors they employ: (1) knowledge factors – "something the user knows" (passwords, PINs, security questions); (2) possession factors – "something the user has" (hardware tokens, smart cards, mobile devices); and (3) inherence factors – "something the user is" (biometric identifiers such as fingerprints or facial recognition) [1]. While this tripartite model remains fundamental, modern digital ecosystems have extended it with contextual and behavioral factors – "something the user does" or "somewhere the user is" – enabling adaptive authentication based on device location, time, or usage patterns [2].

From a technological perspective, MFA systems can be classified into several distinct categories. TOTP systems generate temporary codes using cryptographic algorithms that are synchronised with server time, offering robust protection against brute-force attacks. SMS-based authentication relies on mobile networks to deliver one-time codes via text messages, offering high accessibility but limited resistance to SIM swapping and interception. Push notification-based authentication sends approval requests to trusted devices, allowing users to confirm login attempts through secure channels. Hardware tokens such as YubiKey and FIDO2 keys, use cryptographic challenge-response methods that offer the strongest protection against phishing and replay attacks [3].

Regarding system architecture, MFA can be implemented as centralised systems with all factors verified by one identity provider like Azure AD or Okta, or as federated systems, where authentication is shared across multiple trusted domains. A hybrid approach often combines both, allowing integration between corporate and cloud environments. Cloud-based MFA services increasingly adopt standards such as FIDO2 and WebAuthn, which eliminate shared secrets and link authentication directly to the domain origin, thereby strengthening resistance to credential theft [4].

To enhance understanding and comparison, a structured taxonomy can be proposed that considers four core dimensions: (1) factor type, (2) delivery channel, (3) cryptographic model, and (4) user interaction. According to this extended classification, TOTP and SMS belong to symmetric key models relying on code transmission or generation, while push notifications and hardware tokens represent asymmetric or challenge-based mechanisms. Comparative evaluation demonstrates that hardware tokens and push-based systems achieve the best balance between security and usability, whereas SMS, despite being widespread, shows the highest exposure to social engineering and network attacks.

A summarized comparison of selected MFA technologies highlights the trade-off between usability and protection. TOTP offers offline functionality but requires synchronization; SMS provides convenience but low resilience; push notifications ensure a good user experience with moderate risk; and hardware tokens guarantee strong cryptographic security with limited accessibility due to cost and device dependency [5].

In conclusion, the proposed systematization and classification of MFA methods demonstrate that effective authentication strategies must combine multiple complementary factors while considering both technological capabilities and user behavior. Future research should focus on developing adaptive MFA architectures that dynamically adjust verification strength based on contextual risk, ensuring both robust protection and practical usability.

References:

1. Stallings W. Cryptography and Network Security: Principles and Practice. Pearson, 2023. 816 p.

2. ENISA. Guidelines on Modern Authentication and Authorization Protocols. European Union Agency for Cybersecurity, 2023. 80 p.

3. NIST. Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B). National Institute of Standards and Technology, 2022. 79 p.

4. FIDO Alliance. FIDO2: Moving the World Beyond Passwords, Technical Overview. FIDO Alliance, 2023. 75 p.

5. Microsoft. Multi-Factor Authentication Overview and Best Practices. Microsoft Corporation, 2024. 10 p.