UDC 004

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

## ANALYSIS OF ATTACK VECTORS AGAINST MULTIFACTOR AUTHENTICATION SYSTEMS

The implementation of multifactor authentication (MFA) has become one of the most effective means of enhancing access control and protecting user accounts from unauthorized access. However, despite the significant improvement in security compared to single-factor systems, MFA mechanisms remain vulnerable to a variety of attack vectors that exploit human, technical, and organizational weaknesses. Analysing these attacks is critical to assessing how well MFA systems perform and identifying areas for improvement.

One of the most common threats is SIM swapping, which targets SMS-based authentication. In this attack, criminals trick mobile carriers into transferring a victim's phone number to a SIM card they control, enabling them to intercept one-time passwords and reset account credentials. This attack is especially dangerous because it circumvents digital security measures by exploiting vulnerabilities in telecom procedures. According to a 2023 FBI report, SIM swapping attacks have resulted in millions of dollars in cryptocurrency theft and identity fraud [1].

Phishing and man-in-the-middle (MITM) attacks represent another major category of MFA threats. Modern phishing tools have advanced beyond basic credential theft pages and now include real-time proxy features that can intercept authentication sessions between users and legitimate services. These sophisticated tools act as invisible intermediaries, capturing both passwords and second-factor codes during the authentication process. Browser-based reverse proxies such as Modlishka or Evilginx2 demonstrate how easily TOTP or push-based MFA can be bypassed when users are tricked into entering their data on a cloned website [2]. Session hijacking and replay attacks also remain relevant: adversaries can intercept valid authentication tokens or cookies and reuse them to impersonate users within active sessions.

A separate category of social engineering attacks exploits human behavior rather than technical flaws. The so-called MFA fatigue or "push bombing" attack overwhelms a user with repeated login prompts until they accidentally or intentionally approve one. According to Microsoft's Digital Defense Report, such attacks accounted for more than 20% of recorded MFA breaches in 2023 [3]. The success of these attacks highlights the need for

adaptive authentication policies that include number matching or contextual verification.

Comparative analysis of attack success rates across authentication methods reveals distinct vulnerability profiles. SMS-based MFA demonstrates the lowest resistance due to interception and SIM swapping, making it unsuitable for high-security environments. TOTP applications such as Google Authenticator provide stronger protection but remain susceptible to phishing-based code theft and replay within short time windows. Push notification systems offer convenience but face behavioral exploitation through fatigue or spoofed approval prompts. In contrast, hardware tokens and FIDO2 security keys provide the highest resistance because they use asymmetric cryptography and bind authentication to specific domains, preventing interception and replay [4].

Statistical data confirm that nearly 80% of successful MFA bypasses occur in systems using SMS or TOTP, while phishing-resistant methods such as FIDO2 account for less than 2% of incidents [5]. Nevertheless, widespread adoption of secure technologies remains limited due to cost, hardware availability, and user convenience factors. Therefore, the challenge lies in achieving a balance between usability and security.

In conclusion, the analysis of attack vectors against MFA systems demonstrates that no method is entirely immune to compromise. Effective protection requires a combination of phishing-resistant protocols, user education, and adaptive risk-based authentication. Future research should focus on developing hybrid mechanisms that integrate behavioral analytics, cryptographic verification, and contextual awareness to dynamically respond to evolving attack strategies.

**References:**

1. FBI; CISA. Public advisory on SIM-swapping attacks. FBI & CISA, 2023. 6 p.

2. Enisa. ENISA threat landscape 2023. European Union Agency for Cybersecurity, 2023. 144 p.

3. Microsoft. Digital defense report 2023. Microsoft Corporation, 2023. 131 p.

4. Cisco Talos. MFA bypass and exploitation report, Q1 2024. Cisco Systems, 2024. 18 p.

5. Verizon. Data breach investigations report 2024. Verizon Communications, 2024. 100 p.