UDC 004.056.523

ENHANCING BROWSER SECURITY: THREATS, MULTI-FACTOR AUTHENTICATION, AND ADVANCED PROTECTION MECHANISMS

Khyzhniak M.A.
mykyta.khyzhniak@nure.ua
Scientific supervisor – Ovcharenko D. R.
Kharkiv National University of Radio Electronics, Dep. CRETISS

This work provides an overview of key cybersecurity threats related to web browsers and the role of multi-factor authentication (MFA) in enhancing security. It examines threats such as phishing attacks, malware, man-in-the-middle (MITM) attacks, and malicious browser extensions. Special attention is given to the development of MFA and its impact on browser security, with a focus on modern authentication standards like WebAuthn and FIDO2, highlighting their advantages over traditional security methods [1, 2] and the need for widespread implementation of MFA.

Modern web browsers are an essential tool for interacting with the internet space; however, they also represent a primary target for cybercriminals. Among the most common threats are phishing, malicious software (malware), man-in-the-middle (MITM) attacks, user tracking, and browser vulnerability exploitation [1].

Phishing is a social engineering technique aimed at deceiving users to obtain their credentials. Cybercriminals create counterfeit web pages that mimic official resources of banks, universities, and scientific organizations. Effective countermeasures against phishing include URL verification, the use of built-in browser protection mechanisms, specialized anti-phishing extensions, and the implementation of multi-factor authentication (MFA) [1].

Malware can infiltrate a system through downloading infected files, exploiting browser vulnerabilities, or installing malicious extensions. To mitigate these risks, it is crucial to regularly update browsers, use antivirus software, and restrict extension access to sensitive data [3].

MITM attacks pose a significant threat, particularly when using public Wi-Fi networks, as attackers can intercept and modify transmitted data. To minimize risks, it is advisable to use VPNs, HTTPS protocols, and secure DNS servers to prevent spoofing attacks [2].

Malicious browser extensions may request excessive permissions, making them a potential risk for data leakage. Therefore, it is critically important to install only verified and official add-ons from trusted sources [3].

Multi-factor authentication (MFA) has evolved to counter modern cybersecurity threats. Initially based on passwords and one-time codes via SMS or email, it proved vulnerable to SIM-skimming and phishing attacks [1]. To enhance security, TOTP generators like Google Authenticator and Authy enabled local code generation, while hardware keys such as YubiKey and Titan Security

Key provided physical account protection [2]. A breakthrough came with biometric authentication (Face ID, Touch ID) and modern standards like WebAuthn and FIDO2, which use cryptographic keys stored on user devices, eliminating password-related risks and improving authentication convenience [3].

Multi-factor authentication (MFA) plays a crucial role in enhancing web browsing security by adding an extra layer of protection for user accounts. Even if cybercriminals gain access to a user's password, account access remains inaccessible without a second verification factor, such as a one-time code, a hardware key, or biometric data [1].

One of the most effective MFA methods is the use of FIDO2 hardware keys, which employ cryptographic authentication techniques. Unlike traditional password-based authentication, these keys are resistant to phishing attacks, as fraudulent websites cannot replicate cryptographic authentication protocols. This significantly enhances the security of browser-based accounts by eliminating the risks associated with password theft [2].

Modern browsers have integrated MFA support, particularly through the WebAuthn standard, which simplifies and accelerates secure account access. The adoption of passwordless authentication mechanisms reduces reliance on passwords, decreasing the risk of credential-based attacks. Additionally, the use of password managers and automated authentication solutions helps mitigate security risks associated with weak or reused passwords [3].

Despite its advantages, MFA adoption still faces challenges, including user reluctance due to perceived complexity and compatibility issues across different platforms and services. Addressing these challenges requires the continuous improvement of authentication technologies and the promotion of user-friendly security practices [1].

Thus, the implementation of multi-factor authentication in browsers serves as a key measure for protecting user data, preventing unauthorized access, and strengthening overall cybersecurity. The integration of advanced authentication methods, such as FIDO2 and WebAuthn, marks a transition towards a more secure and efficient authentication paradigm in web environments [2, 3].

References. 1. Amft, S., Höltervennhoff, S., Huaman, N., Krause, A., Simko, L., Acar, Y., & Fahl, S. (2023). "We've Disabled MFA for You": An Evaluation of the Security and Usability of Multi-Factor Authentication Recovery Deployments. arXiv preprint arXiv:2306.09708. 2. Hackenjos, T., Wagner, B., Herr, J., Rill, J., Wehmer, M., Goerke, N., & Baumgart, I. (2022). FIDO2 With Two Displays–Or How to Protect Security-Critical Web Transactions Against Malware Attacks. arXiv preprint arXiv:2206.13358. 3. Cherry, A., Barmpis, K., & Shahandashti, S. F. (2024). The Emperor is Now Clothed: A Secure Governance Framework for Web User Authentication through Password Managers. arXiv preprint arXiv:2407.07205.