
Security Vulnerabilities and Mitigation Strategies for VPNs and Password Managers: A Comprehensive Review in the Post-Pandemic Threat Landscape

Kirtpreet Kaur, Krishnendu Rarhi, Tarang Gupta

Chandigarh University

Abstract.

The growing reliance on Password Managers (PMs) and VPNs for digital security emphasizes the importance of addressing persistent vulnerabilities, such as plaintext credential leaking in memory (CWE-316), which impacts a wide range of popular applications. As remote work and cyber dangers become more prevalent, future research should focus on expanding security evaluations to mobile platforms and other client-side programs, such as Remote Desktop Protocol (RDP) and Secure Socket Shell (SSH) clients. Further improvements in VPN security, such as AI-driven threat detection, post-quantum cryptography (PQC), zero-trust designs, and intelligent traffic analysis techniques, will be critical for increasing resilience to emerging cyber-attacks.

Keywords. Cyber Security, Password Manager, Ransomware, Virtual Private Network, Vulnerability.

1. INTRODUCTION

In this era of fast digital change, the security of software services and applications is critical. VPNs and PMs are the foundation of end-user security, but recent discoveries reveal a significant flaw in their protective capabilities: the exposing of crucial credentials in plaintext within system memory [1]. This vulnerability allows attackers to obtain high-value passwords, granting illegal access to business infrastructures and frequently culminating in devastating ransomware assaults. The COVID-19 epidemic exacerbated these vulnerabilities by forcing a global shift to remote employment, broadening the attack surface and making VPN infrastructures great targets for cybercriminals [2]. This research looks at these underlying flaws, focusing on the risks caused by persistent plaintext passwords in memory after authentication. By evaluating recent academic and industry studies, we want to uncover hidden credential leaks, examine future attack vectors, and present a paradigm for improving VPN and PM security in today's hostile threat environment.

2. LITERATURE REVIEW

This section highlights the findings from the research work on VPNs and related security tools. Despite their widespread adoption as a "prerequisite toolkit to enhance the end-user

arsenal," a significant portion of PMs and VPN clients are leak sensitive user credentials in plaintext in system memory. Studies shows 75 % of desktop, 100% of browser PMs, 75% of PM plugins, and 33% of VPN apps leak user credentials. These findings highlight CWE-316 as a critical concern that causes phishing and ransomware. The post-COVID-19 boom in remote work increased VPN usage and, as a result, the number of cyberattacks targeting VPN weaknesses and human mistake. Common attack techniques include phishing, ransomware, and DDoS, utilizing MITRE ATTACK tactics like Reconnaissance and Credential Access [2]. WireGuard is noted for its high speed and kernel-level security, while IPsec is recognized for its robust site-to-site protection despite configuration complexities [10]. Applying Spring Security Framework with Key Cloak-Based OAuth2 to Protect Micro service Architecture APIs: A Case Study explores the area of research over how to secure data sharing using APIs in microservice-based systems, focusing more on the healthcare department [8]. The author has designed, implemented, and tested decentralized architecture against a number of tests, using wireless technologies like Starlink and Long-Term Evolution, managed through an SD-WAN platform that enables smart traffic routing and prioritization [5].

Furthermore, the research highlights a significant gap between provider claims and operational reality. Many tunnelling VPN services over-promise privacy while omitting mention of potential threat agents, leading to faulty user mental models [6]. For instance, while "Tor over VPN" is a popular concept among tech enthusiasts, their security can be doubtful [5]. The percentage of tested programs that showed cleartext credential exposure in system memory in at least one assessed scenario is known as the leakage rate. The overall conclusions are predicated on Table 2.1

Application category	Tested	Leakage observed	Leakage (%)	Associated weakness / CVE and affected product
Desktop password managers	12	9	75%	CWE-316; CVE-2023-23349 (Kaspersky Password Manager); CVE-2024-9203 (Enpass Password Manager)
Browser password managers	5	5	100%	CWE-316; aggregate finding reported by the source study
Password-manager browser plugins	12	9	75%	CWE-316; aggregate finding reported by the source study
VPN client applications	21	7	33%	CWE-316; CVE-2024-50570 (FortiClient)

Table 2.1. Summary of Applications Leaking Plaintext Passwords

3. ANALYSIS

The research of the post-pandemic threat landscape indicates a complex combination of technological weaknesses and strategic exploitation. The persistence of plaintext credentials in memory (CWE-316) is a crucial enabler of lateral movement. Attackers with limited rights can use memory dumps to collect credentials, circumventing the CIA triad's protections (confidentiality, integrity, and availability) . This is especially troubling given the 33% rise in VPN usage following COVID-19, which coincided with a 75% spike in daily cybercrime reports from the FBI. Modern attack tactics have evolved to exploit these flaws. State-sponsored APTs now often target reported VPN vulnerabilities (e.g., UNC2717, APT34) using MITRE ATT&CK-based methods, such as reconnaissance, initial access, and

persistence [6]. To address these issues, the researchers propose a multifaceted hardening architecture. This includes implementing Multi-Factor Authentication (MFA) and Access Control Lists (ACLs), as well as adopting current protocols such as SSL, WireGuard, and OpenVPN [4][9]. Advanced encryption techniques, such as CRYSTALS-Kyber, are being integrated to increase resilience to quantum computing threats. Furthermore, the integration of VPNs with Next-Generation Firewalls (NGFW) and the use of honeypots for counterintelligence (e.g., blocking an attacker's VPN via embedded payloads) are proactive changes in defensive strategy. The goal is to shift from passive encryption to an autonomous, decentralized, and intelligent security architecture [7]. Figure 3.1 node size = frequency, links = co-occurrence, colors = thematic clusters. Figure 3.2 node size = citations, links = similarity, colors = year. Figure 3.3 node size = citations, links = citations, layout = recency vs. citation count.

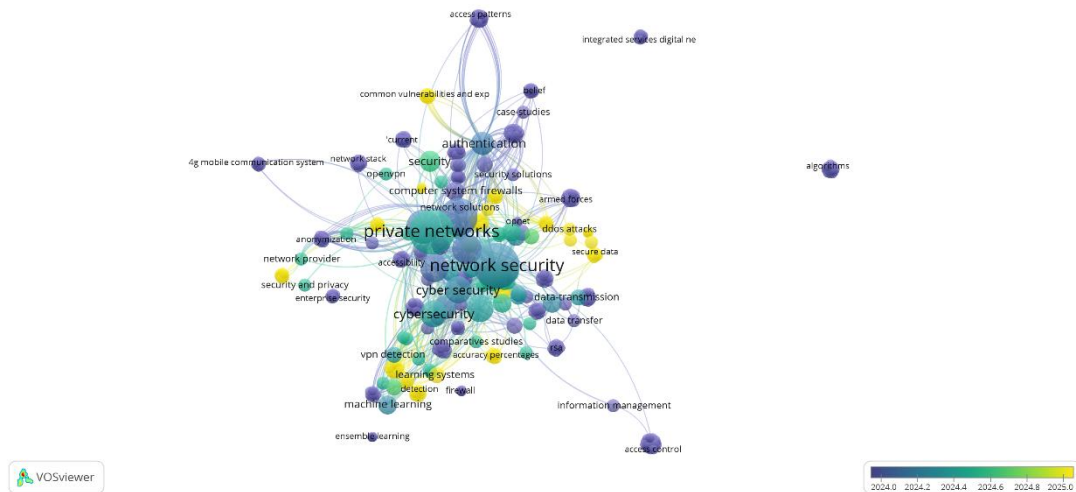


Figure 3.1: Keyword co-occurrence map

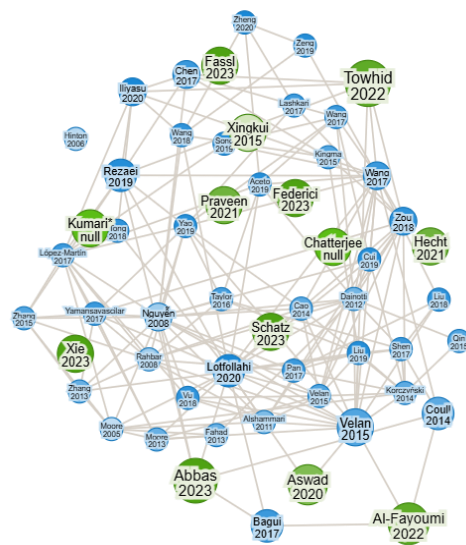


Figure 3.2: Interconnection and thematic similarities among papers

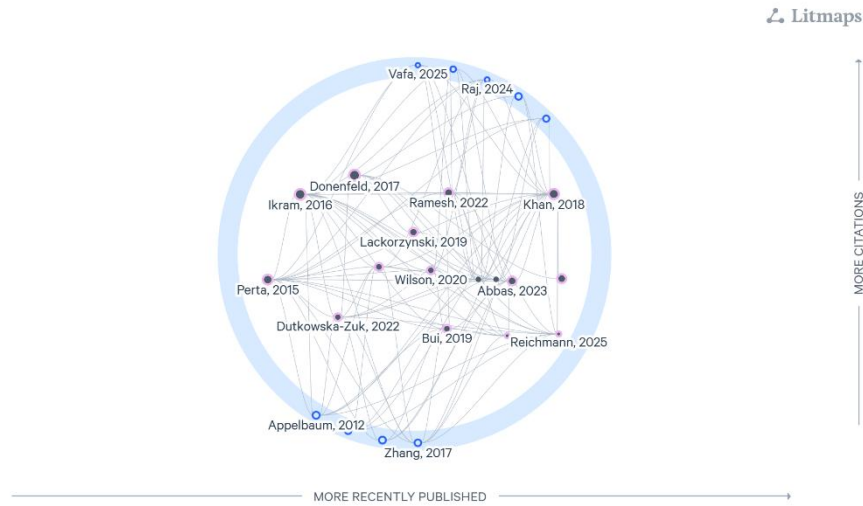


Figure 3.3: Citation network of research papers

4. CONCLUSION AND FUTURE SCOPE

The growing reliance on PMs and VPNs involves addressing vulnerabilities like CWE-316. Future study should include mobile platforms and client-side technologies (RDP, SSH). Enhancements must incorporate AI-driven threat detection, PQC, and zero-trust design to create resilience against emerging threats .

5. REFERENCES

- [1] Sivasangari et al., "Designing a secure and robust virtual private network (vpn) framework for enhanced network communication protection," AIP Conference Proceedings, vol. 3257, no. 1, 2025.
- [2] K. Qollakaj et al., "Cybersecurity of remote work migration: A study on the vpn security landscape post covid-19 outbreak," Array, p. 100437, 2025.
- [3] A. Ostroukh, C. Pronin, A. Podberezkin, J. Podberezkina, and A. Volkov, "Enhancing corporate network security and performance: A comprehensive evaluation of WireGuard as a next-generation vpn solution," in 2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO). IEEE, 2024, pp.
- [4] M. Zain ul Abideen et al., "Vpn traffic detection in SSL-protected channel," Security and Communication Networks, vol. 2019, 2019..
- [5] H. M. Herrera and Y. D. Granada Mahecha, "Secure remote connectivity with Starlink, LTE, and vpn," SSRN working paper, 2025.
- [6] H. Akter et al., "Evaluating performances of vpn tunneling protocols," in TCCE 2021, Springer, 2022.
- [7] H. Abbas et al., "Security assessment and evaluation of VPNs: a comprehensive survey," ACM Computing Surveys, vol. 55, no. 13s, 2023.
- [8] A. Chatterjee and A. Prinz, Applying Spring Security framework with Keycloak-based OAuth2 to protect microservice architecture APIs, Sensors, vol. 22, no. 5, 2022
- [9] NIST, "Guide to SSL VPNs," Special Publication 800-113, 2008.
- [10] A. Ostroukh et al., "Enhancing corporate network security and performance: A comprehensive evaluation of WireGuard," in 2024 SYNCHROINFO, IEEE, 2024.
- [11] Chatzoglou, E., Kampourakis, V., Tsiatsikas, Z., Karopoulos, G., & Kambourakis, G. Unmasking the hidden credential leaks in password managers and VPN clients. Computers & Security, 150, 104298 (2025). DOI: 10.1016/j.cose.2024.104298.