Password Managers: Security Solutions and Vulnerabilities in Modern Authentication

Sam Wang *Team Member*
Nicole Kuo *Team Member*
Caleb Su *Team Member*
Yi Yu *Team Member*
Parkash Singh *Team Member*

***Abstract*—This document is a model and instructions for LaTeX. This and the IEEEtran.cls file define the components of your paper [title, text, heads, etc.]. *CRITICAL: Do Not Use Symbols, Special Characters, Footnotes, or Math in Paper Title or Abstract.**

***Index Terms*—password managers, cybersecurity, authentication, encryption, LastPass breach**

I. Introduction

A. The Password Problem

The exponential growth of digital services has created an unprecedented authentication crisis affecting billions of users globally. According to NordPass's 2023 research, the average individual manages approximately 168 passwords for personal accounts, with enterprise users handling an additional 87 work-related credentials [1]. This overwhelming credential burden has precipitated widespread adoption of insecure password practices that fundamentally undermine digital security infrastructure.

Human cognitive limitations are the primary driver of poor password practices. Miller's seminal research on memory capacity demonstrated that individuals can reliably remember only 7±2 items in short-term memory [2]. When applied to password management, this constraint manifests in several problematic behaviors. Password reuse affects 65% of users according to Google's security research, creating vulnerability chains where a single compromised credential enables cascading account breaches [3]. Users consistently employ predictable patterns, with over 80% of passwords following common structural patterns such as capitalizing the first letter followed by lowercase letters, numbers, and a special character.

The economic and security implications of inadequate password management are staggering. IBM's Cost of a Data Breach Report 2023 identified compromised credentials as the most common initial attack vector, responsible for 19% of breaches with an average cost of $4.45 million per incident [4]. The Verizon Data Breach Investigations Report reveals that over 80% of hacking-related breaches involve either brute force attacks or the use of lost or stolen credentials [5]. These statistics underscore the critical necessity for systematic approaches to credential management that overcome human limitations while maintaining usability.

Traditional password policies have proven demonstrably insufficient. Requirements for periodic password changes, once considered best practice, actually reduce password quality as users make predictable incremental changes. Complex password requirements, while increasing theoretical entropy, often lead users to write passwords down or store them insecurely, creating new vulnerabilities. Microsoft Research found that strict password policies can decrease overall security by encouraging users to merely satisfy minimum requirements rather than create genuinely strong passwords [6].

B. Motivation and Significance

Password managers have emerged as the primary technological solution to the authentication crisis, fundamentally transforming how individuals and organizations approach credential security. These tools address the core tension between security and usability by automating the generation, storage, and retrieval of complex passwords, effectively removing human memory as a limiting factor in authentication security.

The significance of password managers extends far beyond mere convenience. Research by the University of Cambridge demonstrated that users adopting password managers increase their average password strength by 3.5 times and virtually eliminate password reuse [7]. Modern password managers incorporate advanced security features including breach monitoring, secure password sharing, and multi-factor authentication integration, creating comprehensive security ecosystems rather than simple storage solutions.

Market adoption has accelerated dramatically, driven by high-profile breaches and increased security awareness. The password management software market reached $2.05 billion in 2022 and is projected to grow to $7.13 billion by 2030, representing a compound annual growth rate of 16.8% [8]. Enterprise adoption has been particularly strong, with 57% of IT decision-makers reporting organization-wide password manager deployment as of 2023 [9].

However, the centralization of credentials in password managers introduces new risk considerations. These tools become high-value targets for sophisticated attackers. The LastPass incidents of 2022 highlighted how implementation vulnerabilities can compromise even well-designed security architectures. The OneLogin breach of 2017 and the Passwordstate incident of 2021 further illustrate that password managers are not immune to compromise [10].

The academic and industry research community has responded by developing enhanced security architectures and protocols. Zero-knowledge encryption schemes ensure that

service providers cannot access user passwords even if their systems are compromised. Secure Remote Password (SRP) protocols enable authentication without transmitting passwords over networks. Hardware security module integration provides additional protection for master keys. These technological advances represent significant progress, though implementation challenges remain [11].

II. Technical Background

Password managers rely on a combination of modern cryptography, secure key-management protocols, and architectural design principles to protect user credentials at scale. This section provides an overview of the core technical mechanisms that enable secure password storage, focusing on (1) encryption methods, (2) master password protocols and key derivation, and (3) architectural differences between local and cloud-based systems.

A. Encryption Methods

At the foundation of every password manager is an encrypted vault that stores sensitive user data, including login credentials, secure notes, credit-card information, and identity documents. Modern password managers typically protect this vault using symmetric-key cryptography, most commonly the Advanced Encryption Standard (AES), and specifically AES-256 in Galois/Counter Mode (GCM) for both confidentiality and integrity guarantees [17].

AES-256 encryption is performed entirely on the user's device. Cloud-based password managers do not receive plaintext data; instead, they store only ciphertext produced locally on the client. This design supports a *zero-knowledge* security model, meaning the service provider cannot access vault contents even if the provider is compromised. The overall strength of AES encryption depends directly on the secrecy and strength of the encryption key that unlocks the vault, which is derived from the user's master password through secure key-derivation mechanisms.

B. Master Password Protocols and Key Derivation

Users cannot reasonably memorize or provide a 256-bit cryptographic key directly. Instead, password managers employ a *Key Derivation Function* (KDF) to transform a human-chosen master password into a strong, high-entropy encryption key. Common KDF algorithms include PBKDF2, scrypt, and the more modern Argon2id [18], [19].

KDFs strengthen a potentially weak or guessable password by applying:

- a randomly generated salt,
- a large number of computational iterations,
- memory-hard operations (in the case of Argon2).

The derived key is then used as the AES-256 encryption key for the vault. The derivation workflow can be summarized as follows:

$$\text{Master Password} \xrightarrow{\text{KDF (e.g., PBKDF2/Argon2)}} \text{256-bit Key}$$

$$\text{256-bit Key} \xrightarrow{\text{AES-256}} \text{Decrypted Vault}$$

A strong KDF significantly increases the cost of brute-force attacks, even when attackers obtain an encrypted vault file. The importance of rigorous key derivation was highlighted in the 2022 LastPass breach, where inadequate PBKDF2 iteration counts in older accounts made certain vaults more susceptible to offline cracking attempts.

C. Architectural Differences: Local vs. Cloud-Based Password Managers

Password managers vary in how they store and synchronize encrypted vaults. Broadly, they fall into two categories: *local-only* and *cloud-synchronized* systems.

Local-Only Password Managers: Tools such as KeePass store the encrypted vault exclusively on a user's device. Synchronization, if desired, must be performed manually through file transfer methods such as USB drives or cloud storage services like Dropbox or Google Drive. This model reduces dependence on third-party providers and minimizes cloud-related attack surfaces, but places greater responsibility on the user to maintain backups and manage multi-device access.

Cloud-Based Password Managers: Cloud-based systems, including Bitwarden, 1Password, LastPass, and Dashlane, automatically synchronize encrypted vaults across all user devices. All encryption and decryption occur locally, and only ciphertext (along with encrypted synchronization metadata) is uploaded to the provider's servers. This design enables *end-to-end encrypted synchronization*, where providers store but cannot decrypt user data.

Cloud synchronization enhances usability and multi-device access but introduces additional risks, including cloud breaches, account compromise, and metadata exposure. Nonetheless, strong client-side encryption and proper key derivation significantly mitigate these risks.

III. Comparative Analysis

A. LastPass

LastPass, founded in 2008, represents one of the most widely adopted password management solutions with over 33 million users and 100,000 business customers as of 2023 [12]. The service pioneered many now-standard features including browser-based vault access, automated form filling, and secure note storage. However, recent security incidents have significantly impacted its reputation and market position.

The technical architecture employs AES-256 bit encryption with PBKDF2-SHA256 for key derivation, defaulting to 600,000 iterations as of 2023. The service implements a zero-knowledge security model where encryption and decryption occur locally on user devices. LastPass offers comprehensive platform support including native applications for all major operating systems and browser extensions. The Security Challenge feature analyzes stored passwords for strength, age, and reuse, providing actionable recommendations. Multi-factor authentication options include authenticator apps, hardware keys supporting FIDO2/WebAuthn, and proprietary Grid Authentication.

The August 2022 breach involved unauthorized access to the development environment, with attackers subsequently accessing customer vault data in November 2022. While password vaults remained encrypted, the exposure of unencrypted metadata including URLs and the potential for offline brute-force attacks against vaults with weak master passwords raised serious security concerns. This incident highlighted critical implementation vulnerabilities and the importance of strong master passwords with high PBKDF2 iteration counts [13].

Pricing has evolved significantly, with the free tier severely limited in March 2021. Premium plans start at $3 per user per month for individuals, with business plans ranging from $4 to $7 per user per month depending on features and support requirements.

B. 1Password

1Password, developed by AgileBits since 2006, has established itself as a premium password management solution with an unblemished security record. The service maintains over 15 million users and 100,000 business customers including IBM, Slack, and GitLab [14].

The security architecture employs a unique dual-key encryption system combining the master password with a 128-bit Secret Key generated during account creation. This approach ensures that even if servers are compromised, encrypted data remains protected without the Secret Key. The service uses AES-256-GCM for vault encryption and PBKDF2-SHA256 with 650,000 iterations for key derivation. The Secret Key adds 128 bits of entropy, making brute-force attacks computationally infeasible even with weak master passwords.

Unique features include the Watchtower security monitoring system providing breach alerts and vulnerable password identification, and Travel Mode allowing users to remove sensitive vaults from devices when crossing borders. The service offers exceptional family sharing capabilities with individual vaults for each family member plus shared vaults for common credentials. Business plans include advanced features such as Secrets Automation for DevOps teams, enabling secure credential management in CI/CD pipelines.

1Password's pricing reflects its premium positioning with no free tier available. Individual plans cost $2.99 per month billed annually, family plans supporting up to 5 members cost $4.99 per month, and business plans start at $8 per user per month.

C. Bitwarden

Bitwarden, launched in 2016 as an open-source password manager, has rapidly gained adoption among security-conscious users valuing transparency and flexibility. With over 3 million individual users and 50,000 organizational customers, Bitwarden's open-source model allows independent security audits and self-hosted deployments [15].

The technical architecture employs AES-256 bit encryption in CBC mode with HMAC authentication, PBKDF2-SHA256 with a configurable iteration count (600,001 default, user-adjustable up to 2,000,000), and RSA-2048 for sharing features. The zero-knowledge architecture ensures end-to-end encryption with no server-side decryption capability. Being fully open-source, all code is available on GitHub for review and contribution, with regular third-party security audits publicly published.

The free tier provides exceptional value including unlimited password storage, sync across unlimited devices, and basic two-factor authentication. Premium features include advanced 2FA options, encrypted file attachments up to 1GB, and vault health reports. Self-hosting options enable complete control over data storage, critical for organizations with strict compliance requirements. Bitwarden Send enables secure, temporary sharing of text and files with end-to-end encryption.

Bitwarden's pricing emphasizes accessibility with a generous free tier. Premium individual plans cost $10 per year, family plans supporting 6 users are $40 per year, and enterprise plans at $5 per user per month add SSO, directory sync, and advanced policies.

D. Dashlane

Dashlane, founded in 2012 in Paris, has positioned itself as a comprehensive digital identity protection platform beyond traditional password management. With over 15 million users across 180 countries, Dashlane emphasizes user experience and integrated security services [16].

The security architecture uses AES-256 encryption in GCM mode providing authenticated encryption, Argon2id for key derivation offering superior resistance to GPU and ASIC attacks, and a patented architecture using elliptic curve cryptography for secure sharing. The zero-knowledge architecture is augmented with U2F and FIDO2 support for hardware-based authentication.

Dashlane's feature set extends beyond password management to comprehensive digital protection. The integrated VPN service provides privacy protection on public networks. Dark web monitoring covers billions of records across criminal forums and databases. Identity restoration support assists U.S. users in case of identity theft. The Password Health score provides actionable insights with automated password change capabilities for supported sites. The patented password changer works across hundreds of popular websites.

No free tier has been available since 2022. Individual premium plans cost $4.99 per month billed annually including VPN and dark web monitoring. Family plans at $7.49 per month support up to 10 members. Business plans start at $8 per user per month with enterprise plans requiring custom quotes.

E. Feature and Security Comparison

A comprehensive comparison reveals distinct strengths and trade-offs informing selection decisions for different use cases and security requirements.

Security architecture analysis shows 1Password's Secret Key provides additional entropy significantly strengthening security against server breaches. Dashlane's Argon2id offers superior resistance to parallel attacks compared to PBKDF2.

Bitwarden's open-source model enables independent verification but requires careful evaluation of self-hosted deployments. LastPass's recent breaches highlight the importance of implementation security beyond cryptographic primitives.

Feature differentiation reflects varying philosophies in password management. Dashlane integrates VPN and identity protection services for comprehensive security. 1Password's Travel Mode addresses specific threat models around border crossings. Bitwarden's Send feature enables secure credential sharing without requiring recipient accounts. LastPass's automated password changing, while limited, reduces friction in credential rotation.

Usability considerations significantly impact adoption. 1Password consistently receives highest ratings for interface design and onboarding. Bitwarden's identical functionality across platforms ensures consistent experience. Dashlane's automatic password changer works reliably across the widest range of websites. LastPass's browser-centric design appeals to users primarily working in web environments.

Value propositions vary across market segments. Bitwarden's generous free tier provides exceptional value for budget-conscious users. 1Password's premium features and security architecture justify higher pricing for security-focused users. Dashlane's bundled services appeal to users seeking comprehensive digital protection. LastPass's enterprise features remain strong despite recent security incidents.

The selection decision ultimately depends on specific requirements, threat models, and constraints. Individual users prioritizing security should consider 1Password's Secret Key architecture or Bitwarden's transparency. Organizations with compliance requirements may prefer Bitwarden's self-hosting or 1Password's security track record. Users seeking comprehensive protection might choose Dashlane's integrated services. Budget-conscious users will find Bitwarden's free tier compelling.

IV. Security Vulnerabilities & Case Studies

A. LastPass 2022 Breach (Primary Case Study)

The 2022 LastPass incident represents one of the most consequential breaches involving a commercial password manager and illustrates how weaknesses in implementation and operations can undermine strong cryptographic design. LastPass experienced two related security incidents during 2022 that ultimately resulted in the exfiltration of customer vault backups, unencrypted metadata, and internal technical information [13]. This case study highlights how attacker focus on development environments, cloud storage configuration, and legacy settings can create systemic risk in password manager deployments.

The initial intrusion in August 2022 began with the compromise of a LastPass developer's endpoint. The attacker exploited a vulnerable third-party media software package installed on the developer's personal machine, gained code execution, and then used captured credentials and multi-factor authentication tokens to access the LastPass development environment. During this phase, the adversary exfiltrated portions of proprietary source code and internal documentation but did not yet access customer vault data. However, the stolen information provided detailed insight into the company's architecture, network topology, and security controls, laying the groundwork for a more extensive compromise [13].

In a second phase disclosed in December 2022, the same threat actor leveraged knowledge from the earlier breach to target LastPass's cloud infrastructure. By abusing credentials and keys obtained from the development environment, the attacker accessed an Amazon Web Services (AWS) S3 bucket that stored encrypted customer vault backups and related data. While the contents of individual vaults, including passwords and secure notes, remained encrypted with AES-256 derived from each user's master password, large volumes of unencrypted metadata were exposed. This metadata included website URLs, folder names, and some form-fill data, which can be highly sensitive because it reveals which services each user relies on and supports targeted phishing and credential-stuffing attacks [13].

A central security concern raised by the incident is the reliance on user-chosen master passwords and key derivation parameters to withstand offline brute-force attacks. LastPass employs a zero-knowledge model in which vault encryption and decryption occur on the client side, and master passwords are never transmitted to the service. The strength of this model depends critically on two factors: the entropy of the master password and the iteration count used with PBKDF2-SHA256 to derive the vault key. Although LastPass increased its default iteration count to 600,000 for new accounts and updated configurations [13], many existing users had legacy settings as low as 5,000 iterations. For these users, weak or reused master passwords significantly lower the cost for attackers to perform offline guessing against the stolen vault backups.

The breach also exposed limitations in LastPass's application of zero-knowledge principles beyond the core vault data. While the encrypted blobs could not be decrypted without user master passwords, the exposure of unencrypted metadata and infrastructure secrets demonstrates that "zero knowledge" at the cryptographic layer does not automatically translate into zero knowledge at the system level. The ability of attackers to move laterally from a compromised developer machine to cloud storage containing production backups indicates insufficient segmentation, monitoring, and key management between development and production environments. From a security architecture perspective, the incident underscores that protecting a high-value target such as a password manager requires rigorous hardening of supporting systems, not only strong client-side encryption.

From the perspective of this paper, the LastPass 2022 breach illustrates both the strengths and weaknesses of modern password manager designs. On one hand, properly configured vaults with strong, unique master passwords and high PBKDF2 iteration counts remain resistant to practical decryption, even after large-scale data exfiltration. On the other hand, the incident demonstrates that implementation details, legacy configuration choices, and operational practices can materially erode the security guarantees that password managers aim

to provide. Effective deployment therefore requires not only robust cryptography but also secure development practices, strict separation of environments, continuous configuration hardening, and user education about master password strength and key derivation settings.

B. Other Notable Vulnerabilities

While the 2022 LastPass breach is the most prominent recent incident, other password managers and the broader ecosystem have exhibited serious weaknesses that reveal recurring design and implementation pitfalls. Academic analyses of password managers demonstrate that even when strong cryptography is used, subtle web and UI logic flaws can undermine security guarantees. Real-world incidents further show that server-side compromise, supply-chain attacks, and local side-channel vulnerabilities all pose significant risks to users of these tools [20], [21].

Early systematic evaluations revealed that many commercial password managers were vulnerable to web-based attacks that bypassed their cryptographic safeguards. Silver et al. showed that multiple tools would autofill credentials into non-TLS pages, attacker-controlled iframes, or scripts injected via cross-site scripting (XSS), enabling credential theft even though vault contents were securely encrypted at rest [20]. Li et al. later demonstrated that browser-integrated "cloud" password managers suffered from origin mismatches, incomplete URL comparison, and DOM confusion, allowing cross-site credential extraction in several services [21]. Together, these studies highlight that autofill policies and origin checking are as critical to security as the underlying encryption.

Beyond LastPass, other enterprise password managers have suffered high-impact breaches that reveal significant architectural trade-offs. In 2017, OneLogin disclosed that attackers had obtained the ability to decrypt some customer data by compromising keys stored in its infrastructure, illustrating the dangers of server-side possession of decryption material for centrally hosted vaults [22]. In April 2021, Click Studios' Passwordstate experienced a supply-chain attack in which a malicious software update delivered a backdoor to customers, allowing exfiltration of stored credentials and system metadata [23]. Subsequent analyses emphasized that Passwordstate's server-centric design, which lacked strict client-side encryption for sensitive data, allowed attacker-controlled code to decrypt passwords directly on customers' servers [27].

Local-only password managers are not immune to serious flaws. In 2023, CVE-2023-32784 revealed a vulnerability in KeePass 2.x allowing extraction of the master password from a memory dump, even when the database was locked or KeePass was no longer running, due to predictable in-memory password handling [25]. Public proof-of-concept implementations further demonstrate near-cleartext reconstruction of master passwords from RAM artifacts [26]. These findings underscore that even password managers with strong cryptography can be compromised by unsafe memory management and insufficient resistance to forensic recovery.

Finally, several incidents highlight that password managers can also be compromised indirectly through account-level attacks such as credential stuffing. In early 2023, Gen Digital reported that thousands of NortonLifeLock password manager accounts were taken over when attackers reused passwords from unrelated breaches to access vaults lacking multi-factor authentication (MFA) [24]. While the underlying cryptographic design remained intact, the incident illustrates that password managers function as high-value authentication hubs: without strong MFA, anomaly detection, and rate limiting, attackers may compromise all downstream accounts.

Collectively, these incidents demonstrate that password manager security depends on far more than strong ciphers or key-derivation functions. Secure origin validation, safe autofill logic, robust server-side key management, protected update channels, hardened memory handling, and resilient account-level protections such as MFA all play critical roles. These insights inform the common vulnerability patterns discussed in the following subsection.

V. Conclusion and Discussion

A. Best Practices and Recommendations

B. Future of Password Management

C. Role in Broader Cybersecurity Landscape

References

[1] NordPass, "Juggling security: How many passwords does the average person have in 2024?," Apr. 2024. [Online]. Available: https://nordpass.com/blog/how-many-passwords-does-average-person-have/. Accessed: Nov. 12, 2025.

[2] G. A. Miller, "The magical number seven, plus or minus two: Some limits on our capacity for processing information," *Psychological Review*, vol. 63, no. 2, pp. 81–97, 1956. doi: 10.1037/h0043158.

[3] Google Security Team, "New research: How effective is basic account hygiene at preventing hijacking," Google Security Blog, May 17, 2019. [Online]. Available: https://security.googleblog.com/2019/05/new-research-how-effective-is-basic.html. Accessed: Nov. 12, 2025.

[4] IBM Security, *Cost of a Data Breach Report 2023*. IBM Corporation, Jul. 2023. [Online]. Available: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs. Accessed: Nov. 12, 2025.

[5] Verizon, *2023 Data Breach Investigations Report (DBIR)*. Verizon Enterprise, 2023. [Online]. Available: https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf. Accessed: Nov. 12, 2025.

[6] D. Florêncio and C. Herley, "Where do security policies come from?," in *Proc. 6th Symposium on Usable Privacy and Security (SOUPS)*, 2010, pp. 1–14. [Online]. Available: https://cups.cs.cmu.edu/soups/2010/proceedings/a10_florencio.pdf. (Corrected year: 2010.)

[7] S. Pearman, S. A. Zhang, L. Bauer, N. Christin, and L. F. Cranor, "Why people (don't) use password managers effectively," in *Proc. 15th Symposium on Usable Privacy and Security (SOUPS)*, 2019. [Online]. Available: https://www.usenix.org/system/files/soups2019-pearman.pdf. (Corrected venue/year: SOUPS 2019.)

[8] Grand View Research, *Password Management Market Size & Trends Report*. Grand View Research, Inc., 2023. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/password-management-market. Accessed: Nov. 12, 2025.

[9] Forrester Research, "Best Practices: Selecting, Deploying, and Managing Enterprise Password Managers," 2023. [Online]. Available: https://omnibus.healthcareinfosecurity.com/whitepapers/forrester-report-best-practices-selecting-deploying-managing-w-4143. Accessed: Nov. 12, 2025.

[10] OneLogin, “Security incident,” May 2017. (Coverage) B. Krebs, “OneLogin breach exposed ability to decrypt data,” *KrebsOnSecurity*, Jun. 2017. [Online]. Available: https://krebsonsecurity.com/2017/06/onelogin-breach-exposed-ability-to-decrypt-data/. Accessed: Nov. 12, 2025.
[11] T. Wu, “The SRP authentication and key exchange system,” RFC 2945, Internet Engineering Task Force (IETF), Sep. 2000. [Online]. Available: https://www.rfc-editor.org/rfc/rfc2945.html. (Corrected year: 2000.)
[12] LastPass and FIDO Alliance, *The 2023 Workforce Authentication Report: Embracing the Passwordless Future*. 2023. [Online]. Available: https://www.lastpass.com/-/media/2a928b6acd804afa9e699bb4c262cc14.pdf. Accessed: Nov. 12, 2025.
[13] LastPass, “Notice of recent security incident,” Dec. 22, 2022. [Online]. Available: https://blog.lastpass.com/posts/notice-of-recent-security-incident. Accessed: Nov. 12, 2025.
[14] 1Password, “Company overview,” Company web page, 2023. [Online]. Available: https://1password.com/company. Accessed: Nov. 12, 2025.
[15] Bitwarden Inc., “About Bitwarden,” Company web page, 2023. [Online]. Available: https://bitwarden.com/about/. Accessed: Nov. 12, 2025.
[16] Dashlane Inc., “Company overview,” Company web page, 2023. [Online]. Available: https://www.dashlane.com/about. Accessed: Nov. 12, 2025.
[17] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering*. Wiley, 2010.
[18] J. Bonneau, “The science of guessing: Analyzing an anonymized corpus of 70 million passwords,” in *Proceedings of the IEEE Symposium on Security and Privacy*, 2012.
[19] A. Biryukov, D. Dinu, and D. Khovratovich, “Argon2: The memory-hard function for password hashing and other applications,” Password Hashing Competition Report, 2016.
[20] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, “Password Managers: Attacks and Defenses,” in *Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14)*, 2014.
[21] Z. Li, W. He, D. Akhawe, and D. Song, “The Emperor’s New Password Manager: Security Analysis of Web-based Password Managers,” Technical Report No. UCB/EECS-2014-138, University of California, Berkeley, 2014.
[22] B. Krebs, “OneLogin: Breach Exposed Ability to Decrypt Data,” KrebsOnSecurity, Jun. 2017.
[23] HIPAA Journal, “PasswordState Password Manager Supply-Chain Attack,” *HIPAA Journal*, May 2021.
[24] (ISC)^2, “The LastPass Breach: Are Online Password Managers Still Safe?,” *(ISC)^2 Insights*, Feb. 2023.
[25] National Institute of Standards and Technology, “CVE-2023-32784: KeePass 2.x Master Password Recovery from Memory,” *National Vulnerability Database*, May 2023.
[26] V. Dohny, “KeePass 2.X Master Password Dumper (CVE-2023-32784),” GitHub repository, 2023.
[27] Cyberis, “Exploiting KeePass CVE-2023-32784,” Cyberis, Oct. 2024.