Survey on Web Authentication and Security

Swetha Mohan
swethamohan@umass.edu
University of Massachusetts Amherst

Amanda Arcieri
aarcieri@umass.edu
University of Massachusetts Amherst

Mariana Jaramillo
mjaramillo@umass.edu
University of Massachusetts Amherst

Abstract

Web authentication is undergoing a major transition driven by large-scale deployment of passwordless mechanisms, increased adoption of phishing-resistant multi-factor authentication, and widespread use of federated identity protocols. Between 2019 and 2024, top security venues have published a growing body of work analyzing the security, usability, and real-world effectiveness of these systems. This survey presents a structured review of over 24 representative papers from CCS, NDSS, IEEE S&P, USENIX Security, and PETs, covering passwordless authentication (WebAuthn, FIDO2, passkeys), multi-factor authentication, single sign-on protocols, session management, and phishing resistance. We synthesize findings across these domains, compare approaches based on security guarantees, usability, deployability, and ecosystem support, and identify emerging trends such as the ecosystem-driven push for passkeys and the shift toward phishing-resistant authentication. We further highlight open gaps, including limited longitudinal deployment studies, inconsistent usability evaluations, and unresolved tensions between security and user experience. Finally, we outline promising research directions for designing robust, usable, and widely deployable web authentication systems.

1 Introduction

Authentication remains a foundational component of web security, directly impacting user privacy, account safety, and the resilience of online services to large-scale attacks. Despite decades of research, passwords continue to be a dominant authentication mechanism, even as they are repeatedly shown to be vulnerable to phishing, credential reuse, and large-scale compromise. In response, the web ecosystem has seen rapid adoption of alternative mechanisms such as multi-factor authentication (MFA), federated identity systems, and, more recently, passwordless authentication based on WebAuthn and FIDO2 standards.

From 2019 to 2024, research published in top security venues has increasingly focused on evaluating these modern authentication mechanisms in practice. This period coincides with major industry shifts, including browser-level WebAuthn support, large-scale deployment of phishing-resistant hardware tokens, and ecosystem-wide promotion of passkeys by Apple, Google, and Microsoft. At the same time, new attacks on single sign-on (SSO) protocols, token-based authentication systems, and session management mechanisms continue to surface, highlighting that eliminating passwords alone does not eliminate authentication risk.

This survey aims to provide a comprehensive and structured overview of recent research on web authentication systems. Rather than proposing a new authentication mechanism, we synthesize and compare existing work across multiple dimensions: security guarantees, usability tradeoffs, deployability, and real-world effectiveness against threats such as phishing and session hijacking. We organize the literature into five core categories: passwordless authentication, multi-factor authentication, federated identity and SSO, session management, and phishing resistance, and analyze each category using a common framework.

We provide a unified taxonomy and summary of recent web authentication research across major security venues. We compare and rank authentication approaches based on practical criteria, identifying strengths, weaknesses, and tradeoffs. We highlight gaps in existing work and outline open research challenges, particularly around usability, deployment friction, and long-term security guarantees.

2 Passwordless Authentication

Passwordless authentication has emerged as a promising alternative to traditional password-based systems, aiming to reduce susceptibility to phishing, credential reuse, and large-scale credential breaches. Standards such as WebAuthn and FIDO2 enable public-key–based authentication tied to user devices, shifting authentication secrets from shared knowledge to cryptographic keys protected by hardware and platform security. More recently, major ecosystem players like Apple, Google, and Microsoft, have promoted passkeys as a user-friendly abstraction over FIDO2, enabling seamless cross-device authentication. This section reviews recent research evaluating the security, usability, and deployment challenges of these passwordless approaches.

Several studies focus on security guarantees and attack surfaces of FIDO2-based authentication. *A Security and Usability Analysis of Local Attacks Against FIDO2* (NDSS 2024)[1] systematically examines local adversaries who gain temporary or partial access to a user's device. The paper demonstrates that while FIDO2 effectively mitigates remote phishing attacks, local attacks such as malware-assisted key usage or biometric bypasses, remain feasible under certain conditions, particularly when platform authenticators rely on weak user verification mechanisms. The study highlights a tension between usability and security: relaxing user verification (e.g., allowing fallback PINs or weak biometrics) significantly increases attack success rates. These findings emphasize that FIDO2's security benefits are not absolute and depend heavily on platform-level enforcement and configuration.

User understanding and mental models of passwordless authentication are explored by Lassak et al. in *"It's Stored, Hopefully, on an Encrypted Server"* (USENIX Security 2021)[2]. Through user studies, the authors reveal widespread misconceptions about how WebAuthn and FIDO2 operate, with many users incorrectly believing that biometric data or credentials are stored remotely. Such misunderstandings affect trust, adoption, and user decision-making, particularly around recovery and device loss. Similarly, *Is FIDO2 the Kingslayer of User Authentication?* (IEEE S&P)[3] provides a comparative usability evaluation, showing that while FIDO2 can outperform passwords in authentication speed and perceived security, it introduces new usability challenges related to device dependency, account recovery, and cross-platform consistency. These studies collectively demonstrate that usability remains a critical barrier to widespread adoption despite strong cryptographic foundations.

Deployment and ecosystem challenges are further examined in *Why Aren't We Using Passkeys? Obstacles Companies Face Deploying FIDO2 Passwordless Authentication*[4], which highlights organizational hesitations including integration complexity, legacy system compatibility, support costs, and uncertainty around user support and recovery flows. While passkeys aim to simplify FIDO2 adoption through platform-level integration and cloud-backed synchronization, the paper suggests that enterprise adoption is slowed by operational concerns rather than purely technical limitations. In parallel, *Let's Authenticate: Automated Certificates for User Authentication* (NDSS 2022)[5] explores an alternative passwordless direction using automated certificate issuance, demonstrating the feasibility of public-key authentication without user-managed secrets, but raising questions about certificate lifecycle management and trust anchors. Extending beyond web contexts, *From Hardware Fingerprint to Access Token* (NDSS 2024)[6] investigates passwordless authentication on IoT devices, illustrating how hardware-bound identities can enhance security in constrained environments, albeit with limited usability evaluation.

Across these works, several advantages of passwordless authentication are consistently identified: strong phishing resistance, elimination of shared secrets, and improved protection against credential reuse. However, the limitations are equally clear. Local attacks, usability breakdowns during device loss or recovery, user misconceptions, and organizational deployment barriers remain significant challenges. Notably, most studies evaluate authentication in controlled or short-term settings, leaving gaps in understanding long-term usability, recovery behavior, and failure modes at scale.

Future research directions include developing more robust user verification mechanisms resilient to local compromise, improving user education and mental models, and designing recovery processes that balance security with accessibility. Additionally, studies of passkey adoption across diverse user populations and enterprise environments are needed to validate whether ecosystem-driven deployment can overcome current barriers. Overall, while passwordless authentication represents a substantial step forward, existing research suggests it should be viewed as an evolving system rather than a complete replacement for all password-based authentication scenarios.

3 Multi-Factor Authentication

Multi-factor authentication (MFA) has been brought forth to be used as a defense against phishing, and password compromise by requiring users to authenticate through multiple factors. This is done through something they know, something they have or something they are. Common MFA mechanisms are SMS-based authentication, time-based one-time password (TOTP) applications, push notifications and hardware security keys. Recent research has shown that its real-world effectiveness heavily depends on the deployment of this authentication mechanism's usability, consistency, and the security.

TOTP-based authentication in the paper, *Security and Privacy Failures in Popular 2FA Apps* (USENIX Security 2023)[7] examines the practical security of this deployed MFA method. The authors of this paper present a comprehensive analysis of back up and recovery mechanisms in 22 popular Android TOTP applications. There is demonstration of violations of basic security principles, such as allowing plaintext backups of TOTP secrets, flawed encryption and insecure cloud transmission of sensitive data. While the protections are put in place to reinforce this authentication mechanism, their poor implementation results in ineffective protections. The backup systems rely on insecure recovery channels such as email or SMS, which ultimately undermine MFA itself. While TOTP is theoretically secure, insecure implementation choices in backup and recovery systems completely undermine it.

Usability and consistency issues are highlighted in, *A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites* (NDSS 2023)[8]. The authors analyze the lifecycle of 2FA, which include, discovery, setup, usage and deactivation across 85 popular websites. They discovered the inconsistencies of how MFA is presented and managed. 2FA usability varies drastically across these websites, in naming conventions, device remembrance, recovery options and deactivation warnings. This results in users having to relearn MFA for each website which discourages adoption. These inconsistencies impact user experience and directly impact security, as this may cause users to disable or avoid MFA altogether.

The authors of *A Study of Multi-Factor and Risk-Based Authentication Availability* (USENIX 2023)[9] provide a big-picture view of fewer than half of major sites actually supporting MFA, despite being widely recommended. 208 major websites were evaluated, and their implementation of MFA and risk-based authentication (RBA). RBA mechanisms often failed to block suspicious login attempts, specifically, most sites recognized a suspicious login, but did not block them. The fallback mechanisms put in place, such as email or SMS, undid the security that MFA provided. However, the authors observed that popular platforms offering a third-party single sign-on (SSO) provided stronger authentication protections. This suggests that centralized identity providers often outperform site-specific MFA deployments. There is a greater understanding and awareness of MFA's importance, but its adoption and implementation remains inconsistent.

This paper explores the transition from traditional MFA toward phishing-resistant authentication methods with FIDO2. *From TOTPs to Security Keys: Studying the Reality of Passwordless FIDO2 Authentication With PIN And Biometrics in a Corporate Environments* (SOUPS 2025)[10] examines the adoption of FIDO2-based authentication as a way to replace traditional MFA. This research compares the TOTP-based methods with the hardware-backed FIDO2 credentials, while focusing on passwordless authentication. FIDO2-based authentication was found to significantly reduce the phishing risk and user friction but introduces challenges related to user understanding, device dependency and recovery processes. Users often misunderstand how PINS and biometrics functions within web authentication which reinforce the broad theme that usability are critical determinants of authentication security.

Recurring strengths and weaknesses of MFA are the undeniable improvement of security over password-only authentication. MFA still remains a critical line of defense against large-scale credential compromise. MFA's effectiveness is undermined by insecure backup and recovery mechanisms. There are inconsistent user experiences, weak fallback channels and partial or optional deployment. SMS-based MFA remains widely used due to its convenience and usability. However, it offers limited protection against modern phishing attacks. TOTP apps provide stronger guarantees but still suffer from vulnerabilities due to flawed backups and developer errors. MFA do show promise, but face low adoption and inconsistencies across platforms.

Future research includes strengthening MFA without reintroducing weak authentication journeys, standardizing usability to reduce confusion and accelerating adoption of FIDO2, and other phishing-resistant MFA. Studies are needed to understand how users interact with

MFA long-term, with incidents such as device loss or account recovery. Existing research suggests that MFA is not an overall solution but a collection of authentication mechanisms with careful design, standardized deployment and alignment between usability and threat models.

4 Single Sign-On

Single sign-on (SSO) streamlines user authentication through delegating identity verification to trusted third-party providers or other identity providers (IdPs). Standards like OAuth 2.0 and OpenID Connect (OIDC) underpin most SSO deployments. This enables service providers to authenticate users without handling credentials directly. In theory, SSO enhances usability and can centralize authentication policies, but it also introduces new obstacles. These range from protocol implementation correctness to the amount of user data shared during authentication.

AuthSaber: Automated Safety Verification of OpenID Connect Programs (CSS '24)[11] develops automated analysis tools to check the correctness of OpenID Connect Implementations against formal safety specifications. Modern SSO systems built on OIDC may have subtle bugs that can undermine guarantees assumed by the protocol. The authors design and apply an automated verifier to express safety properties to check whether widely used OIDC libraries satisfy these safety requirements. Their evaluation has uncovered previously known vulnerabilities in prominent libraries. This demonstrates the deviations that may exist in prominent libraries resulting in detrimental vulnerabilities. SSO security depends on the correctness of implementation, which can be a challenge given the complexity of real-world authentication software and deployment.

There are privacy implications of OAuth-based SSO when deployed across a large number of sites, and this is examined in *Everybody's Looking for SSOmething: A Large-Scale Evaluation on the Privacy of OAuth Authentication on the Web*[12]. The authors analyze which data scopes websites request from identity providers and how often these go beyond the minimal need for authentication. A significant fraction of these websites request non-minimal OAuth scopes without actual dependence on the extra information. Excessive scopes request personal user data like location, and users lack control which scopes they grant. OAuth-based SSO often exposes more user data than necessary, these findings suggest. Which may result in the enabling of cross-site tracking and violation of data.

Several trends and gaps still persist in the scale of modern SSO adoption. Privacy leaks remain widespread due to the lack of user data minimization and user control. OIDC implementations are shown to be buggy which can lead to vulnerabilities. These issues demonstrate the implementation and usability of SSO comes along with nuanced risks due to security flaws and privacy leakage.

Future research must show either side of this issue, improved tools and workflows that verify OIDC and OAuth codebases. Additionally, there must be mechanisms that reduce the amount of data leakage and include user consent in this process. This can balance functionality with privacy. Integrating privacy preservation can reduce the amount of data exposed without sacrificing the usability benefits of SSO. SSO plays a critical role in web authentication, but privacy and security remain areas of concern that require further attention to maintain or even explode the attractiveness of SSO.

5 Session Management and Cookies

Session management remains a critical yet fragile component of web authentication, serving as the bridge between initial authentication and sustained user identity across requests. Despite advances in authentication mechanisms, failures in session handling such as insecure cookie configurations, token leakage, and flawed account creation workflows continue to enable account compromise. Recent research from 2019–2024 highlights that even when strong authentication is used, weaknesses in session management can undermine overall system security. This section surveys key attacks and defenses related to cookies, SameSite policies, and token-based authentication mechanisms such as OAuth 2.0 and JWTs.

Several works expose fundamental flaws in session initialization and account creation workflows. *Pre-hijacked Accounts: An Empirical Study of Security Failures in User Account Creation on the Web* (USENIX Security 2022) demonstrates that attackers can preemptively create accounts using victim email addresses before legitimate users register, enabling persistent session hijacking and identity confusion. The study reveals that many websites fail to adequately verify email ownership during account creation, allowing attackers to bind sessions or authentication tokens to victim identities. Crucially, these attacks bypass traditional authentication defenses, illustrating that session security depends not only on login mechanisms but also on secure identity binding and lifecycle management.

Cookie-based session handling is further scrutinized in *Cookie Crumbles: Breaking and Fixing Web Session Integrity*, which systematically analyzes how misconfigured cookies such as missing Secure, HttpOnly, or SameSite attributes, enable session fixation and session hijacking attacks. The paper shows that attackers can manipulate session identifiers during authentication flows, especially in multi-step login or OAuth-based authentication processes. While proposed fixes emphasize stricter cookie attribute enforcement and server-side session binding, the authors note that backward compatibility and inconsistent browser behavior complicate widespread deployment of these defenses.

The introduction of the SameSite cookie attribute was intended to mitigate cross-site request forgery (CSRF) and limit cross-site cookie leakage. However, *The State of the SameSite* (IEEE S&P) provides a large-scale empirical evaluation of SameSite deployment and effectiveness across the web. The study finds widespread misconfiguration, incomplete adoption, and misunderstandings of SameSite semantics among developers. Notably, the paper shows that SameSite alone does not fully prevent session leakage in complex authentication flows involving redirects, embedded resources, or legacy browser behaviors. These findings suggest that browser-enforced defenses are necessary but insufficient without correct developer usage and complementary server-side checks.

Beyond cookies, token-based authentication systems introduce their own attack surfaces. *Universal Cross-app Attacks: Exploiting and Securing OAuth 2.0 in Integration Platforms* reveals how OAuth tokens can be misused across applications within integration platforms, enabling attackers to pivot between services using leaked or overly permissive access tokens. The paper highlights common vulnerabilities such as improper token scoping, reuse of authorization codes, and lack of audience restriction in JWTs. These flaws are particularly concerning given the widespread reliance on OAuth 2.0 and OpenID Connect for SSO and API authentication, where token compromise can lead to broad account and data exposure.

Across these studies, several strengths and limitations of existing session management approaches emerge. Cookie-based sessions benefit from mature browser support and well-understood security properties, but remain vulnerable to misconfiguration and complex authentication flows. Token-based systems offer scalability and flexibility but increase the risk of token leakage, overprivileged access, and cross-application abuse. A recurring theme is that defenses such as SameSite cookies and OAuth best practices are effective in theory but frequently undermined by inconsistent implementation and evolving attack strategies.

Significant research gaps remain in understanding the long-term effectiveness of session defenses in real-world deployments. Many studies identify vulnerabilities through large-scale measurements or controlled experiments but lack longitudinal evaluation of how fixes are adopted over time. Additionally, limited work examines user-visible consequences of session failures, such as silent account takeover or persistent identity confusion. Future research should focus on unified session integrity models that span authentication, account creation, and token lifecycle management, as well as automated tools to detect and prevent session misbinding and token misuse at scale. Overall, the surveyed work underscores that securing authentication requires equal attention to the often-overlooked session layer.

6 Phishing Resistance

Phishing resistance is the ability of authentication systems and surrounding account ecosystems to prevent attackers from obtaining usable credentials or authentication proofs even when users are deceived. Phishing resistance requires not only cryptographic protections but also deployment choices, recovery flows, and interfaces that do not reintroduce weaker, replayable factors. It also depends on usability and user mental models, since defenses that users misunderstand or fail to adopt provide little protection.

Across the surveyed papers, key findings show that phishing resistance frequently breaks at the human layer rather than at the cryptographic layer. The authors of *Why Users (Don't) Use Password Managers at a Large Educational Institution* (USENIX 2022)[13] demonstrate that password managers improve password hygiene and reduce reuse, especially when third-party managers are adopted. However, ease of use is the factor that drives that adoption. Additionally, the study in *Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols* (USENIX 2021)[14] shows that FIDO is cryptographically resistant to phishing. However, real deployments permit fallback methods that attackers can socially engineer users into using. In *A Transcontinental Analysis of Account Remediation Protocols of Popular Websites* (USEC 2023)[15], the authors prove that websites worldwide provide inconsistent and incomplete remediation guidance. This issue creates opportunities for post-phishing exploitation. Additionally, the authors of *Cryptographic Deniability: A Multi-perspective Study of User Perceptions and Expectations* (USENIX 2023)[16] show that users misunderstand properties such as cryptographic deniability and the authors of P*hishing Attacks against Password Manager Browser Extensions* (USENIX 2025)[17] show that those users can be tricked by spoofed password manager extension UIs into revealing master passwords. Lastly, the study in *Phish in Sheep's Clothing: Exploring the Authentication Pitfalls of Browser Fingerprinting* (USENIX 2022)[18] shows that users are also vulnerable to browser fingerprinting attacks that allow phishing sites to bypass multifactor authentication.

The advantages throughout these studies demonstrate that phishing resistance is achievable in theory. Password managers, particularly dedicated third-party ones, reduce password reuse and support strong and unique credentials which limit the effectiveness of credential harvesting attacks[13]. Second, FIDO provides strong origin binding that prevents token relay attacks central to real-time phishing[14]. Additionally, clear remediation guidance and recovery processes can reduce attacker leverage after compromise and help users recover safely[15]. Also, insights into user misconceptions about deniability and trust highlight where UX improvements can harden systems against social engineering[16]. Lastly, password managers and browser signals can add protective layers when properly designed and deployed[17].

However, the papers in this survey also reveal significant limitations that weaken phishing resistance in practice. First, FIDO's protection is undermined by widespread fallback and recovery mechanisms vulnerable to social engineering[14]. Second, many users rely on superficial cues and fail to detect subtle phishing indicators which means strong authentication[16]. Additionally, browser embedded password manager UIs are easily impersonated which nullifies their phishing resistance advantages[17]. Another limitation is that browser fingerprints act as replayable tokens that attackers can harvest and reuse to bypass multifactor authentication invisibly[18]. Lastly, incomplete remediation guidance further amplifies damage once phishing succeeds[15].

Several gaps remain in the existing research. There is little longitudinal measurement of how combined defenses such as password managers, phishing resistant authenticators, and remediation practices change phishing success rates over time. There are also limited studies that explore unforgeable or cryptographically verifiable UI elements that cannot be replicated within webpage content. Additionally, cross factor interactions such as password managers, fingerprinting, and recovery flows remain underexplored. Lastly, there is limited research in regional and language differences in user understanding of remediation and security cues.

Future work should aim to close these gaps through coordinated advances in both research and system design. A key direction is the development of account recovery flows that preserve phishing resistance, such as device attested recovery or tightly verified human support processes that do not rely on easily coerced fallback mechanisms. At the interface level, stronger separation between browser chrome and web content is needed to prevent convincing impersonation of trusted UI elements, particularly for password managers . From an organizational perspective, institutions can meaningfully improve security by incentivizing the adoption of secure and usable third-party password managers through provisioning and training. Finally, authentication systems should move away from replayable signals like browser fingerprints toward nonextractable authentication factors that attackers cannot clone via phishing.

In conclusion, the surveyed papers demonstrate that phishing resistance is not a standalone property of cryptography or authentication protocols, but an ecosystem shaped by usability, interfaces, and recovery design. Strong cryptography like FIDO is necessary but insufficient if usability, fallback mechanisms, remediation practices, and user understanding undermine it. Usable security drives adoption, misunderstood guarantees enable social engineering, and UI and fingerprinting design choices can inadvertently aid attackers. A layered approach of combining usable password managers, phishing resistant authenticators, hardened recovery flows, and clear remediation guidance offers the most realistic path to reducing phishing success in practice.

References:

1. Tarun Kumar Yadav and Kent Seamons. 2024. A Security and Usability Analysis of Local Attacks Against FIDO2. In Network and Distributed System Security Symposium (NDSS)
2. Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur. 2021. "It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn. In USENIX Security Symposium.
3. Lyastani, Sanam Ghorbani; Schilling, Michael; Neumayr, Michaela; Backes, Michael; Bugiel, Sven (2020). Is FIDO2 the Kingslayer of User Authentication? A Comparative Usability Study of FIDO2 Passwordless Authentication. CISPA. Conference contribution. https://doi.org/10.60882/cispa.24613269.v2
4. Leona Lassak, Elleen Pan, Blase Ur, and Maximilian Golla. 2024. Why aren't we using passkeys? obstacles companies face deploying FIDO2 passwordless authentication. In Proceedings of the 33rd USENIX Conference on Security Symposium (SEC '24). USENIX Association, USA, Article 404, 7231–7248.
5. Conners, J., Devenport, C., Derbidge, S., Farnsworth, N., Gates, K., Lambert, S., McClain, C., Nichols, P., & Zappala, D. 2022. Let’s Authenticate: Automated Certificates for User Authentication. In Proceedings of the Network and Distributed System Security Symposium (NDSS)
6. Xiao, Y., He, Y., Zhang, X., Wang, Q., Xie, R., Sun, K., Xu, K., & Li, Q. 2024. From Hardware Fingerprint to Access Token: Enhancing the Authentication on IoT Devices. In Proceedings of the Network and Distributed System Security Symposium (NDSS). The Internet Society.
7. Conor Gilsenan, Fuzail Shakir, Noura Alomar, and Serge Egelman. 2023. Security and privacy failures in popular 2FA apps. In Proceedings of the 32nd USENIX Conference on Security Symposium (SEC '23). USENIX Association, USA, Article 117, 2079–2096.
8. Shihan Lin, Suting Chen, Yunming Xiao, Yanqi Gu, Aleksandar Kuzmanovic, and Xiaowei Yang. 2025. PreAcher: secure and practical password pre-authentication by content delivery networks. In Proceedings of the 22nd USENIX Symposium on Networked Systems Design and Implementation (NSDI '25). USENIX Association, USA, Article 75, 1399–1419.
9. Anthony Gavazzi, Ryan Williams, Engin Kirda, Long Lu, Andre King, Andy Davis, and Tim Leek. 2023. A study of multi-factor and risk-based authentication availability. In Proceedings of the 32nd USENIX Conference on Security Symposium (SEC '23). USENIX Association, USA, Article 115, 2043–2060.
10. Leona Lassak, Nicklas Lindemann, and Marvin Kowalewski. 2025. From TOTPs to security keys: studying the reality of passwordless FIDO2 authentication with PIN and biometrics in a corporate environment. In Proceedings of the Twenty-First USENIX Conference on Usable Privacy and Security (SOUPS '25). USENIX Association, USA, Article 21, 371–389.
11. Tamjid Al Rahat, Yu Feng, and Yuan Tian. 2024. AuthSaber: Automated Safety Verification of OpenID Connect Programs. In Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security (CCS '24). Association for Computing Machinery, New York, NY, USA, 2949–2962. https://doi.org/10.1145/3658644.3670318
12. Dimova, Y., Van Goethem, T., & Joosen, W. 2023. Everybody’s Looking for SSOmething: A Large-Scale Evaluation on the Privacy of OAuth Authentication on the Web. Proceedings on Privacy Enhancing Technologies, 2023(4), 452–467.
13. Mayer, P., Munyendo, C. W., Mazurek, M. L., & Aviv, A. J. 2022. *Why Users (Don’t) Use Password Managers at a Large Educational Institution.* In 31st USENIX Security Symposium (USENIX Security ’22), Boston, MA, USA, 1849–1866. (USENIX)
14. Ulqinaku, E., Assal, H., Abdou, A. R., Chiasson, S., & Capkun, S. 2021. *Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols.* In 30th USENIX Security Symposium (USENIX Security ’21), Virtual Event, 3811–3828. (USENIX)
15. Markert, P., Adhikari, A., & Das, S. 2023. *A Transcontinental Analysis of Account Remediation Protocols of Popular Websites.* In Proceedings of the Symposium on Usable Security and Privacy (USEC ’23). (arXiv)
16. Yadav, T. K., Gosain, D., & Seamons, K. 2023. *Cryptographic Deniability: A Multi-perspective Study of User Perceptions and Expectations.* In 32nd USENIX Security Symposium (USENIX Security ’23), Anaheim, CA, USA, 3637–3654. (USENIX)

17. Anliker, C., Lain, D., & Capkun, S. 2025. *Phishing Attacks against Password Manager Browser Extensions.* In 34th USENIX Security Symposium (USENIX Security ’25), Seattle, WA, USA. (USENIX)

18. Lin, X., Ilia, P., Solanki, S., & Polakis, J. 2022. *Phish in Sheep’s Clothing: Exploring the Authentication Pitfalls of Browser Fingerprinting.* In 31st USENIX Security Symposium (USENIX Security ’22), Boston, MA, USA, 1651–1668. (USENIX)