What happened at Okta?

Ram Larg
2120398

Prompt 2: Discuss the human security and societal impact factors involved in the Okta support hack.

1 Events leading up to the attack and its impact

On October 2nd, 2023, a BeyondTrust Okta administrator uploaded an HTTP Archive (HAR) file[†] at the request of Okta customer support to troubleshoot an ongoing support issue [1]. Thirty minutes after the upload, a malicious actor was able to use the session cookie obtained from this HAR file in an attempt to access the BeyondTrust Okta admin console. The attack method the threat actor uses is consistent with accounts from other companies affected by this attack, reporting a session hijacking using customer support tickets [2, 3].

According to BeyondTrust's blog report, the attacker accessed an authenticated account by leveraging this acquired session cookie [1]. Once authenticated, they tried to access the console but were denied due to a policy requirement of having installed Okta Verify on managed devices. The attacker resorted to using API actions as these could not be protected by the same policies used for the admin console. To impersonate existing service accounts, the attacker then creates a backdoor user account, 'svc_network_backup' [1]. BeyondTrust immediately deactivates the backdoor account upon detection through the security system before internal damage could be caused. There is insufficient evidence from other sources that can confirm the attack methods on BeyondTrust to this detail. Critically, we must consider the limited perspective that this report provides. Despite this, the report expressed details of BeyondTrust's indicators of compromise that included an IP address Okta used to identify the compromised service account [4], giving the source real credibility. The website also presents a strong history of reporting on security topics dating back to 2010 [5], as well as this particular instance having been written by the Chief Technology Officer of BeyondTrust Marc Maiffret.

BeyondTrust eliminated the possibility of compromise originating from their own systems after investigation, contacting Okta support on October 3rd to escalate concerns to the Okta security team that they may have been compromised [1]. At this point, there had been no communication from Okta about a possible

[†]A JSON-formatted archive file logging a web browser's interaction with a website.

breach [4]. BeyondTrust and Okta then held a call on October 11th and 13th to discuss findings but still received no confirmation from Okta about a possible breach. It was not until October 19th that BeyondTrust received official notification from Okta Security that there was, in fact, a breach in their systems. This interchange is supported by a statement released from Okta's Chief Security Officer Bradbury, who detailed a similar communication timeline with Okta not alerting their customers for approximately two weeks after initial reports of suspicious behaviour [4]. Bradbury defended the delay by elaborating on the period of fourteen days between communications, saying Okta "did not identify any suspicious downloads" in their log files [4]. The attacker was able to view support files without detection from the customer support system by viewing the files indirectly from another tab. As previously mentioned, Okta was able to identify and disable the compromised service account by using BeyondTrust's provided IP address, declared in their IOCs [1]. While the immediate impact of the attack may have been mitigated by Okta's eventual response of revoking the session tokens contained within the HAR files, some suggest it had been too slow [6].

Despite its detail, the report above from BeyondTrust [1] fails to explain how exactly the intruder compromised the Okta customer support system. The report describes a timeline of actions the intruder performed but, for some actions, does not detail how. For example, the attacker was able to access BeyondTrust's HAR file [1] but there is no information about how the attacker was able to accomplish this. The reason for this lack of information may be BeyondTrust's attempt at keeping the report concise and contained. In this respect, BeyondTrust had recently made a report one week prior [7] outlining recent attack flows made against Okta. On the other hand, the official report from Okta describes the intrusion in more depth, with the attacker being able to access the customer support system by compromising an employee's personal Google account or device, on which the employee had saved the username and password of an Okta service account [4]. From the service account, the attacker could access the support system and view all customer support files. Described as the "most likely avenue" by which the attacker gained access to the system [4], it is still up for speculation how the threat actor truly broke into the service account.

There is insufficient evidence to identify precisely how the Okta employee account or device was compromised. However, around the same time in October, BeyondTrust had previously uploaded a report breaking down recent attack flows against Okta [7]. It should be noted that BeyondTrust links to this resource in their recent blog post detailing the latest Okta attack [1]. Assuming the attack flow used may be related or even similar, we can evaluate comparable features between both attack methods. Figure 1 illustrates how previous attack flows against Okta first obtained admin credentials. This attack flow is similar to the most recent attack in that the threat actor had access to the credentials of a service account for the Okta support system. These credentials are

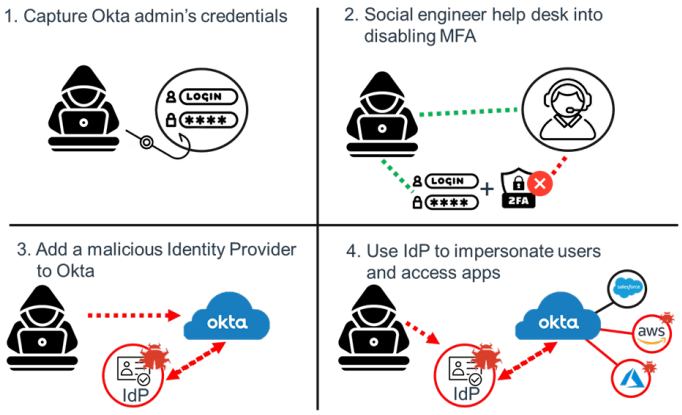

Figure 1: A previous Okta attack flow. Source: BeyondTrust [7].

described to likely have been obtained through phishing[†] [7], which could be an explanation for the root cause of the most recent attack. Part two of the attack flow references socially engineering the help desks into resetting multi-factor authentication (MFA). Reports from the most recent attack have no details of the attacker using social engineering to bypass MFA, only stating that access to the customer support system was acquired by the service account [4]. Part three follows similarly to Okta's most recent attack mentioned in the reports above, where the attacker attempts to gain access to a high-privilege admin role but fails, and the fourth step does not occur.

A comment made by Stanley S on a Krebs on Security forum post about the Okta attack said "We should go with the assumption that information in the support tickets for all Okta clients would have been touched and ex-filtered by the attacker, given that they had access to it (the customer support system) for two weeks" [6, 4]. Although this comment was made by an unknown author on October 24$^{\text{th}}$, their suspicions would be all but confirmed on November 29$^{\text{th}}$ when Okta's CSO Bradbury, released an official update detailing how the attacker was able to download a report containing information on all the names and email addresses of Okta customer support system users [8]. The update from Okta details how 99.6% of users only had their name and email address in the report, but this still leaves open a large vector for attack on the users affected. Additionally, a small number of customers may now have personal details such as their phone number or address accessible to the threat actor, as shown in Table 1. Appropriately, Bradbury also outlines how Okta customers may now be susceptible to phishing and social engineering attacks and heavily proposes that all customers should now utilise MFA. Bradbury discloses 94% of their customer administrators already employ MFA, leaving 6% of their 17,000 customers [9] (approximately 1020) vulnerable to social engineering attacks.

[†]Where attackers deceive people into revealing sensitive information or installing malware.

While the remaining companies onboard MFA, it would be wise to also consider the difficulty of this process. OWASP outlines MFA increasing the complexity for administrators, end users and potentially companies more generally who might find it challenging to integrate MFA into their systems quickly [10]. The businesses impacted by this attack are ultimately the ones who needed Okta's support the most and are currently the ones receiving the most pressure from being vulnerable to attack.

Created Date	Last Login	Full Name	Username	Email
Company Name	User Type	Address	[Date of] Last Password Change or Reset	Role: Name
Role: Description	Phone	Mobile	Time Zone	SAML Federation ID

Table 1: Report fields downloaded by the threat actor. Source: Okta [8].

2 Security considerations and tensions

A security consideration related to the attack is the lack of data sanitisation in the company HAR files. The session hijacking attack on BeyondTrust's side boils down to the attacker acquiring Okta session cookies from the confidential HAR file, allowing the intruder to bypass MFA [1]. The report briefly mentions that Okta recently updated its knowledge base articles on how to sanitise these HAR files [11]. Still, this documentation fails to provide a human-usable way to perform this step, only recommending the use of a text editor to remove sensitive information such as cookies and session tokens*. The documentation by itself in no way fits the task to the human [12], taking into account the potential user or their device's capabilities and limitations. In hindsight, this attack may have been prevented for BeyondTrust and other Okta customers had there been a tool such as Cloudflare's HAR file sanitiser [13], which was developed in response to this breach. This tool strips out any session-related cookies for the user by a simple upload of the HAR file and a selection of options to sanitise. However, the tool still requires user input. Systems should aim to be secure by default [14], so the load of security is not pushed back onto users. Recent developments show some requesting the ability to sanitise these sensitive HAR files by default through the browser [15], allowing this mechanism to be automated further. With HAR files being a common way to troubleshoot network and authentication issues [16, 17], enabling an option to save such files

*The Okta documentation has been updated as of now to offer automatic sanitisation on uploads to their support portal, but our default sanitisation point still holds.

without sensitive data by default might have prevented the recent Okta attack and future attacks on different companies.

A further security consideration connected to the attack is Okta's policy of handling service accounts. Service accounts are those that represent non-human users [18]. They provide a way to manage machine-to-machine authentication and authorisation. Additionally, these service accounts enable a provisioning flow that does not allow for MFA [19]. Thus, organisations need to consider the best security practices in managing such accounts. This could include preventing users from signing into accounts other than those provided by their organisation [20]. Had the Okta employee been blocked by a policy requirement, they would not have been able to save the service account's username and password onto their personal account. Another strongly encouraged practice from Google is not having passwords for service accounts at all but rather using service account keys [18]. These service account keys, like the password, are considered a high-security risk if leaked. Using other means of authentication is recommended, such as impersonating the service account with user credentials where possible. Prior identity authentication is needed in service account impersonation, as opposed to service account keys, which do not require this [18]. In this way, the problem of leaking the service account password could have been overcome.

There is also an apparent tension between service accounts and usability. As Okta's service accounts are required for performing actions on behalf of a user [19], it is in contradiction with Okta's usual interest that an employee should have had access to such an account [4]. Okta has no open-source documentation on user-managed service accounts, but Google Cloud describes them as attached service accounts [21]. A specified service account can be "attached" to a resource, meaning that the resource uses the service account as its identity. Then, once the resource needs access to other resources, it can use the attached service account for authentication. Although not explicitly documented, there are similarities to Okta's definition, where service accounts are expressed as allowing Okta to authenticate data access or perform actions [19]. Assuming the Okta employee was using an attached service account, the reason they were given access to it would make sense, as these can be user-managed. As mentioned before, service account passwords can be even more valuable to attackers than a leaked password as they do not require authentication on sign-on [22].

Thus, the management of these sensitive service account credentials falls down to the user. A user may have to define an expiration time for their service account details when temporary access is required for a resource [18]. This could pressure the user if they end up needing more than the set amount of time. Users might also become responsible for setting up and rotating the service account passwords. Both of these solutions would require more cognitive load for the user managing the service account. Given a choice, most users would take extra physical workload over mental workload [12], which may lead to steps being skipped in this security process. Service accounts are typically not used by humans and, therefore, not designed to be human-usable. It would be beneficial to have Conditional Access policies for service accounts, particularly in cases where users may need access [23]. Such policies would restrict access to IP

addresses within a certain range, ensuring a safe and secure environment [23].

Okta has taken visible steps to remediate its policy issues. For example, the use of configuration options to enable the blocking of personal profiles on Okta-managed devices [4]. Despite their amendments, one could consider it a failure that a substantial identity and access management company, such as Okta [9], cannot properly manage their employee accounts. For Okta, the hole in their security was at the organisational level. Although the one employee could be considered responsible for not noticing the sync between personal and service accounts, Okta's policy controls are undoubtedly at fault - policies that may have prevented the attack at its root. This appears to be a widely held sentiment [24] that Okta's security system design in no way seemed to account for human error [12].

MFA is another security consideration linked to the Okta hack. The case presents itself as requiring stronger authentication on the accounts managed by Okta and its customers. MFA is a security measure that, by definition, involves a combination of more than one distinct authentication method. The three authentication methods described by NIST are something you know, something you have, and something you are [25]. By using these, a company can increase its security by, for example, using software to generate Time-based One-Time Password tokens (TOTP) to authenticate users. As these tokens are generated on another device, it is usually impossible for a threat actor to attack remotely [10]. As mentioned before, Okta released a post detailing the urgency for customers to have MFA to protect the customer support system and the admin consoles for all organisations [8]. BeyondTrust is one such customer with plans to require a robust hardware MFA [1]. They do not specify what type of hardware MFA they plan to use, but we could assume BeyondTrust is planning for FIDO-certified hardware security keys [26]. These can be imagined as physical keys plugged into a device to authenticate the user. A third-party provider of such keys is Yubico [27], a manufacturer of the hardware authentication device YubiKey, as shown in Figure 2.

Figure 2: A YubiKey. Source: Yubico [27].

Hardware MFA is an alternative to passwords that can be added as a layer on top of existing infrastructure, introducing a physical element resistant to phishing attacks. This physical element follows the method of using "something

you have" from the NIST definitions [25]. The advantage of these keys is in the option to eliminate passwords altogether, which could allow the move to a more human-usable environment [12, 28]. Passwords alone can easily be phished and stolen, as demonstrated by the recent attack on Okta. With the advent of Okta's data breach [8], users of Okta's support system now have to be more aware of possible attacks in the coming months. However, a disadvantage of using hardware keys is the vulnerability of loss or having them stolen. Furthermore, physical tokens can incur considerable costs and overhead [10]. Depending on their setup, a stolen hardware key may also be used without a pin or code. Despite these issues, it would be safe to say YubiKeys are still highly effective, reportedly reducing the risk of successful phishing and credential attacks by 99.9% [29]. In addition, according to Forrester, these keys have provided a 203% return on investment (ROI) - suggesting the long-term protection and economic benefits from adopting this security consideration may outweigh the initial costs [29].

It may not be necessary for all Okta support system users to adopt hardware keys as their specific authentication method and could be better off with Bradbury's suggestion of a FIDO2 WebAuthn system [8]. This system also operates on public-key cryptography for authentication but does not require the user to own a hardware key. Instead, WebAuthn allows the user to integrate biometric authentication into web applications and services, providing a smoother MFA login experience and higher security [30]. WebAuthn can include hardware keys such as YubiKeys, but it does not have to; Okta customers can instead opt to use a built-in authentication method on their device, such as face recognition, fingerprint scanning or pin codes [31], which might save additional costs for that company. However, Okta should make an effort to consider such systems themselves. As home to the credential data of thousands of customers [9], Okta naturally invites threat actors who want access to this data. From Yubico and Okta's partnership [32], it is clear that Okta is aware of the advantages of using phishing-resistant MFA through the use of security keys. Okta customers can authenticate easily with YubiKeys without having to worry about software compatibility issues. However, it is clear from the most recent attack [4] that Okta does not appear to have been employing its own security considerations. Suppose the Okta employee - equipped with the service account laptop - faced an authentication policy that included another layer of MFA, such as a hardware key. In that case, the attack may have been mitigated or even stopped entirely.

Usable security is another consideration with regard to the Okta hack. Okta's employee was said to have saved and synced the service account's username and password along with their personal Google account [4]. We can deduce from this that the employee might have been using Google's built-in password manager. This is not unusual, as we know that humans cannot store an infinite number of passwords in their long-term memory (LTM) and may require "coping strategies" to be able to manage all of them [12]. However, that employee was presumably not using Passkeys, a safer, usable and more secure authentication alternative to passwords [33], which was recently released by Google back

on May 3rd, 2023. The fact that the service account credentials on the personal account were the most likely method of compromise contradicts the ethos of a passkey, where public-key cryptography is used to ensure the credentials of accounts cannot be phished or beached in such a manner [34]. Public-key cryptography uses the concept of a key pair: a private key, stored on a user's device and a public key, shared to a website's server [35]. When this pair is created on registration, the private key generated lives on a user's device and is never exposed to any other entity. The public key existing on the server is used to verify a user's identity with a signature challenge using the private key.

The private key behind passkeys could have intercepted the attack on the employee's personal account. Passkeys in the Google password manager are end-to-end encrypted [36], meaning the private key synced to the password manager is only decipherable through an encryption key available on the user's device. For the Okta employee, this may have protected a hypothetical service account passkey from being breached by a malicious attacker. Furthermore, passkeys are much more usable than passwords. On average, authenticating through passkeys is four times more successful than when using passwords [37]. Passkeys have an authentication success rate of 64.8% in comparison to passwords at 13.8%. Passkeys are also usually faster than passwords, with passwords taking twice as long to sign in with at 30.4 seconds and passkeys only taking 14.9 seconds [37]. While there are still concerns towards the security and privacy of the passkey ecosystem, most of them are unfounded [38]. A considerable number of major websites and applications already support some form of passkey [39], making it evident that this security consideration could have played a prominent role in countering the Okta support hack. Reasons as to why Okta may not have been using a passkey pair for its service account are unclear. Like the aforementioned hardware MFA keys, Okta has acknowledged the benefits of passkeys, releasing them as an authentication method for users of their Customer Identity Cloud [40]. Although Okta's own passkey stems from a different company and business model to Google's, both passkeys should conform to the standards outlined by the FIDO Alliance [41]. Both should provide a more usable experience that is faster and more secure than regular passwords. Had Okta been using similar security considerations outlined for their customers, they may have been in a better position to halt the attack on their employee with their designated service account.

It should also be vital to highlight Okta's incident response plan as a security consideration that falls under their organisational behaviours. Between Okta first receiving a report of suspicious activity and its announcement of a breach to its customers, there were around two weeks of silence [4]. After a final investigation, it was discovered that the threat actor had gained access to data on all customers, despite an earlier claim that only 1% of customer support system users were affected one month prior [8]. Based on the evidence, it is apparent that Okta struggles to communicate rapidly with its customers. An interview with Okta's Deputy Chief Information Security Officer Charlotte Wylie reveals initial alerts of compromise were thought not to be due to a fault in Okta's own systems [6]. Likewise, only after reviewing the final investiga-

tion in October did Okta conclude that the threat actor downloaded a report containing data on all support system users [8]. Okta has shown difficulty in maintaining an effective incident response plan. One book by Google on Site Reliability Engineering delineates one of the key hazards in managing incidents is poor communication [42]. Incidents are best declared early, with routine updates to stakeholders. BeyondTrust were forced to have "persisted with escalations" with Okta up until the 19th before the announcement - suggesting Okta were not convinced by initial reports [1]. At least two more customers had to alert Okta support about suspicious activity before they released a notification about a breach [4]. Okta should have been more transparent with their users in this aspect. Okta may have failed in its communication to customers in this event, but it deserves credit for improving its systems' faults and releasing its incident report. It is important to note that Bradbury released a Security Action Plan in October of the previous year [43]. In this plan, Bradbury describes Okta's investment into notification technology and preparing teams to provide rapid responses to stakeholders, actions which could be argued Okta did not hold their word to. Again, we recognise the common theme of Okta bearing the ability and knowledge to have been prepared for the attack but failing at the organisational level to defend itself.

Okta's most recent attack on their support system has highlighted that even well-established identity and access and management companies can have issues with their internal security. Whether due to human factors, technological issues, or organisational-level policies, Okta was not prepared to defend against the attack, let alone anticipate it. The impact of the attack, though initially estimated to be minor, turned out to be far-reaching, affecting all users of the customer support system. Multiple factors contributed to allowing the threat actor to access the system. Although the root cause may have been human error, organisational policies should have accounted for this beforehand. Implementing more usable security standards and appropriate policy restrictions on account privileges could prevent similar attacks in future. What happened at Okta was likely a security attack on an employee. An avoidable attack - had there been just one other security consideration in place.

References

[1] Marc Maiffret. BeyondTrust Discovers Breach of Okta Support Unit, October 2023. URL: https://www.beyondtrust.com/blog/entry/okta-support-unit-breach (visited on 11/20/2023). Backup Publisher: BeyondTrust.

[2] Pedro Canahuati. Okta Support System incident and 1Password — 1Password, 0. URL: https://blog.1password.com/okta-incident/ (visited on 11/28/2023). Section: 1Password.

[3] Multiple Authors. How Cloudflare mitigated yet another Okta compromise, October 2023. URL: http://blog.cloudflare.com/how-cl

oudflare-mitigated-yet-another-okta-compromise/ (visited on 11/28/2023).

[4] David Bradbury. Unauthorized Access to Okta's Support Case Management System: Root Cause and Remediation, November 2023. URL: https://sec.okta.com/articles/2023/11/unauthorized-access-oktas-support-case-management-system-root-cause (visited on 11/20/2023).

[5] BeyondTrust. Blog Archive 2010, December 2010. URL: https://www.beyondtrust.com/blog/archive/2010 (visited on 11/29/2023).

[6] Brian Krebs. Hackers Stole Access Tokens from Okta's Support Unit – Krebs on Security, October 2023. URL: https://krebsonsecurity.com/2023/10/hackers-stole-access-tokens-from-oktas-support-unit/ (visited on 11/28/2023).

[7] James Maude. Identity Attack & Defense: Lessons in Okta Security. URL: https://www.beyondtrust.com/blog/entry/lessons-in-okta-security (visited on 11/20/2023).

[8] David Bradbury. October Customer Support Security Incident - Update and Recommended Actions, November 2023. URL: https://cms.oktaweb.dev/harfiles (visited on 11/29/2023).

[9] Okta. At Work — Technology Industry Trends 2023 — Okta. URL: https://www.okta.com/businesses-at-work/ (visited on 11/21/2023).

[10] OWASP. Multifactor Authentication - OWASP Cheat Sheet Series. URL: https://cheatsheetseries.owasp.org/cheatsheets/Multifactor_Authentication_Cheat_Sheet.html#disadvantages (visited on 11/29/2023).

[11] Okta. Generate HAR files, 2023. URL: https://help.okta.com/oag/en-us/content/topics/access-gateway/troubleshooting-with-har.htm (visited on 11/19/2023).

[12] A Sasse and Awais Rashid. Human factors knowledge area issue 1.0. *The Cyber Security Body of Knowledge*, 2019.

[13] Kenny Johnson. Introducing HAR Sanitizer: secure HAR sharing, October 2023. URL: https://blog.cloudflare.com/introducing-har-sanitizer-secure-har-sharing/ (visited on 11/20/2023). Backup Publisher: The Cloudflare Blog.

[14] NCSC. Secure by Default. URL: https://www.ncsc.gov.uk/information/secure-default (visited on 11/29/2023).

[15] Chromium. Allow & Prefer Saving HAR file without sensitive data - chromium. URL: https://bugs.chromium.org/p/chromium/issues/detail?id=1495801#c6 (visited on 11/29/2023).

[16] Google. Capture web session traffic - Google Ad Manager Help. URL: https://support.google.com/admanager/answer/10358597?hl=en (visited on 11/29/2023).

[17] Auth0. Generate and Analyze HAR Files. URL: https://auth0.com/docs/ (visited on 11/29/2023).

[18] Google. Best practices for managing service account keys — IAM Documentation — Google Cloud. URL: https://cloud.google.com/iam/docs/best-practices-for-managing-service-account-keys (visited on 12/03/2023).

[19] Okta. What Is A Service Account, September 2023. URL: https://support.okta.com/help/s/article/What-Is-A-Service-Account?language=en_US (visited on 11/30/2023).

[20] Google. Block access to consumer accounts - Google Workspace Admin Help. URL: https://support.google.com/a/answer/1668854?hl=en (visited on 11/30/2023).

[21] Google. Attach service accounts to resources — IAM Documentation — Google Cloud. URL: https://cloud.google.com/iam/docs/attach-service-accounts (visited on 12/03/2023).

[22] Google. Best practices for using service accounts — IAM Documentation — Google Cloud. URL: https://cloud.google.com/iam/docs/best-practices-service-accounts (visited on 11/30/2023).

[23] MicrosoftGuyJFlo. Microsoft Entra Conditional Access for workload identities - Microsoft Entra ID, November 2023. URL: https://learn.microsoft.com/en-us/entra/identity/conditional-access/workload-identity (visited on 12/03/2023).

[24] Dan Goodin. No, Okta, senior management, not an errant employee, caused you to get hacked, November 2023. URL: https://arstechnica.com/information-technology/2023/11/no-okta-senior-management-not-an-errant-employee-caused-you-to-get-hacked/ (visited on 11/29/2023).

[25] CSRC Content Editor. MFA - Glossary — CSRC. URL: https://csrc.nist.gov/glossary/term/mfa (visited on 12/01/2023).

[26] FIDO Alliance. How FIDO Works - Standard Public Key Cryptography & User Privacy. URL: https://fidoalliance.org/how-fido-works/ (visited on 12/01/2023).

[27] Yubico. USB-A YubiKey 5 NFC Two Factor Security Key — Yubico. URL: https://www.yubico.com/product/yubikey-5-nfc/ (visited on 12/01/2023).

[28] Yubico. Passwordless Account Login with YubiKey. URL: https://www.yubico.com/solutions/passwordless/ (visited on 12/01/2023).

[29] Forrester. The Total Economic Impact™ Of Yubico YubiKeys. URL: https://tools.totaleconomicimpact.com/go/yubico/yubikeys/?lang=en-us (visited on 12/01/2023).

[30] FIDO Alliance. FIDO2: Web Authentication (WebAuthn). URL: https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/ (visited on 12/02/2023).

[31] Okta. WebAuthn (MFA) — Okta. URL: https://help.okta.com/en-us/content/topics/security/mfa-webauthn.htm (visited on 12/02/2023).

[32] Yubico. Okta Supports Secure Logins With the YubiKey. URL: https://www.yubico.com/works-with-yubikey/catalog/okta/ (visited on 12/02/2023).

[33] Christiaan Brand. The beginning of the end of the password, May 2023. URL: https://blog.google/technology/safety-security/the-beginning-of-the-end-of-the-password/ (visited on 12/02/2023).

[34] Arnar Birgisson. So long passwords, thanks for all the phish, May 2023. URL: https://security.googleblog.com/2023/05/so-long-passwords-thanks-for-all-phish.html (visited on 12/02/2023).

[35] W3C. Web Authentication: An API for accessing Public Key Credentials - Level 2, April 2021. URL: https://www.w3.org/TR/webauthn-2/#credential-key-pair (visited on 12/03/2023).

[36] Arnar Birgisson. Security of Passkeys in the Google Password Manager. URL: https://security.googleblog.com/2022/10/SecurityofPasskeysintheGooglePasswordManager.html (visited on 12/03/2023).

[37] Silvia Convento. Making authentication faster than ever: passkeys vs. passwords, May 2023. URL: https://security.googleblog.com/2023/05/making-authentication-faster-than-ever.html (visited on 12/02/2023).

[38] Dan Goodin. Google passkeys are a no-brainer. You've turned them on, right?, May 2023. URL: https://arstechnica.com/information-technology/2023/05/passwordless-google-accounts-are-easier-and-more-secure-than-passwords-heres-why/ (visited on 12/02/2023).

[39] Hanko. Who supports passkeys? URL: https://www.passkeys.io/who-supports-passkeys (visited on 12/03/2023).

[40] Salman Ladha. Faster, easier, and more secure customer logins with passkeys in Okta, October 2023. URL: https://www.okta.com/blog/2023/10/faster-easier-and-more-secure-customer-logins-with-passkeys-in-okta/ (visited on 12/03/2023).

[41] FIDO Alliance. Passkeys (Passkey Authentication). URL: https://fidoalliance.org/passkeys/ (visited on 12/03/2023).

[42] Betsy Beyer, Chris Jones, Jennifer Petoff, and Niall Richard Murphy. *Site Reliability Engineering: How Google Runs Production Systems*. O'Reilly Media, Inc., 1st edition, March 2016. ISBN: 978-1-4919-2912-4.

[43] David Bradbury. Okta Completes Security Action Plan, October 2022. URL: https://www.okta.com/blog/2022/10/okta-completes-security-action-plan/ (visited on 12/03/2023).