yubico

WEBAUTHN WHITE PAPER SERIES May 2020

Introducing WebAuthn

Enabling a Streamlined and More Secure User Authentication Experience for the Public Sector

Executive Summary

There are many uses cases across the Federal, and State and Local Government where PIV and CAC cards aren't the most suitable authentication method. These include authentication for non PIV/CAC eligible employees and contractors, in isolated networks, authentication for first responders, and for applications and services accessed via mobile devices such as phones and tablets. When public sector entities, intent on improving data security, use SMS text messages as the second factor, they remain vulnerable to SMS hijacking, phishing, and man in the middle (MITM) attacks. Phone-based authentication methods may also put the public sector entity on the hook for mobile cost reimbursement.

WebAuthn, a new web security standard approved by the W3C, offers websites, services, and applications stronger and more user friendly multi-factor authentication, as well as the opportunity to dispense with password-based authentication altogether. WebAuthn is based on public key cryptography that eliminates the need for creating and storing passwords in a central location, where they are vulnerable to data breaches. WebAuthn offers users a wide range of ways to authenticate including the choice of using an external authenticator such as hardware security key or an internal authenticator such as a fingerprint scan. Because public key cryptography enables a website, service, or application to authenticate a user's site-specific credential without storing or sharing the user's private credential itself, it eliminates the risk of stolen passwords, even through phishing attacks. Eliminating passwords also increases productivity while reducing support costs, such as call center costs associated with password-reset requests.

The WebAuthn standard is already supported in all major browsers and most platforms including:

- Windows 10
- Android
- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari
- Apple iOS

Web development teams, as well as security and IT teams responsible for Identity and Access Management and security, should begin looking for products that support the WebAuthn standard, so that employees and partners can benefit from improved security and usability. At the same time, development teams for websites, services, and apps should begin working with the WebAuthn specification, so that they can build support for WebAuthn into their upcoming software releases and offer WebAuthn-supported authentication to users.

Introduction

Cyber-espionage is rampant in the public sector, with state affiliated actors accounting for 79 percent of breaches involving external actors, and privilege misuse and error by insiders accounting for 30 percent of breaches[1]. The use of passwords to access applications and services internally by employees or contractors, and externally by citizens puts public sector entities at risk of being hacked and their data and systems compromised. In addition, forgotten passwords and account lockouts can stack on help desk costs and time.

While PIV and CAC cards are the de-facto authentication standard across a majority of the public sector, they aren't suitable for non PIV/CAC eligible users, in closed gap or isolated networks, for mobile authentication, and for authenticating first responders, volunteers and local constituents.

To stem the flood of leaked data and reinforce their digital bulwarks, web security teams and internal security teams have doubled down on passwords, now requiring them to be more complex, changed more frequently, and reinforced with second authentication factors delivered by text messages or email.

The result: inadequate security and poor user experience.

But now websites, services, and applications have the opportunity to improve both data security and user experience, thanks to a new web authentication standard already supported by web browsers and leading software vendors. The World Wide Web Consortium (W3C), the primary standards body for the Web, has ratified the specification for WebAuthn, a new web authentication standard that simplifies the registration and strengthens the authentication of users for secure interactions with websites, services, and applications[2]. Significantly, WebAuthn takes web authentication beyond the limitations of passwords, improving data security while making login access faster and easier than ever before. All major web browsers and platforms are committed to supporting the WebAuthn standard.

Why WebAuthn Matters

- **Standardization**
  The approval of WebAuthn by the W3C enables the computer industry to standardize strong authentication across browsers and operating systems for the first time.
- **Improved Security**
  WebAuthn raises the bar for web application authentication, improving account security by enabling stronger authentication based on public key cryptography.
- **Streamlined User Experience**
  Web and mobile apps can now easily invoke strong authentication, replacing the hassles of using passwords (and SMS codes[3]) with the convenience of tapping a security key or using a fingerprint scan.
- **User Choice**
  WebAuthn gives users a broad range of choices for authenticating–everything from scanning a fingerprint to entering a PIN to tapping the contact on a hardware security key.
- **Improved Productivity**
  WebAuthn also frees users from the time-consuming and frustrating tasks of hunting for passwords and resetting passwords. This time-savings extends to help desks and support centers who no longer have to devote time to helping users reset passwords.
- **Reduced Costs**
  WebAuthn reduces costs associated with passwords, including productivity costs, support costs, and financial penalties accruing from data breaches perpetrated by attackers using stolen or guessed passwords.

[1] Verizon Data Breach Investigations Report 2019

[2] The W3C has published the protocol specifications here: https://www.w3.org/TR/webauthn/

[3] SMS: Short Message Service, a text-messaging service available on most smartphones and other internet-connected devices. https://en.wikipedia.org/wiki/SMS

- **Accelerated Software Development**
  WebAuthn accelerates software development by enabling developers to implement best-in-class authentication by making registration and authentication calls to the WebAuthn API supported by the browser or platform.

The WebAuthn standard is already supported in:

- Windows 10
- Android
- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari
- Apple iOS

This new standard brings a new level of secure authentication to all internet users. IT organizations should expect WebAuthn-enabled authentication to become available for a growing number of websites, services, and applications in the coming months and years.

Solving the Problems of Passwords and SMS Two-Factor Authentication

To appreciate the importance of WebAuthn, it's helpful to understand the problems with the current state of web authentication. Most authentication today relies on passwords and, in some cases, SMS-based two-factor authentication. Both these approaches have shortcomings for security and user experience.

[4] https://en.wikipedia.org/wiki/Phishing

[5] https://enterprise.verizon.com/resources/reports/2017_dbir.pdf

[6] https://www.yubico.com/authentication-report/

Problems with Passwords

Passwords have been a fact of life—and a source of complaint—for computer users for decades. Problems with passwords include:

Vulnerability to phishing

Phishing continues to be a massive security problem as attack techniques continue to evolve.[4] Attackers send fake email messages urging users to enter their login credentials and then harvest those credentials for account takeovers. Phishing attacks are dismayingly successful. About 30% of phishing emails are opened by their recipients. Over 7% of email recipients are duped into opening an attachment or clicking on a link, which is usually a login link. Most of these attacks eventually lead not only to credentials being stolen but also to the installation of malware for perpetrating a breach.[5] Even if users create complex passwords that are difficult to guess, their accounts can be compromised once hackers harvest their login credentials through phishing.

Stolen credential lists

When hackers break into an organization and steal credentials, they gain access not only to that organization's accounts but also accounts at other organizations where users have used the same username-password pair.

These types of attacks will likely continue as long as websites, services, and applications rely on passwords for account security.

Password fatigue

Users grow tired of creating new passwords for different services and having to change passwords every few months according to the dictates of security policies. To reduce memorization, many users end up re-using passwords across multiple sites or relying on simplistic passwords, which unfortunately are easy to crack. In a Ponemon Institute report, The 2020 State of Password and Authentication Security Behaviors Report, both Individuals and IT security respondents have reused passwords on an average of 10 of their personal accounts.[6] Were any of those passwords to be breached, attackers would gain access to multiple websites and applications.

Password sharing

A password is only secure if it's private. But the 2020 Ponemon Report found that 49% percent of IT security respondents and 51% of Individuals say they are sharing passwords with their fellow employees.[7]

Lost passwords and costly support requests

When users forget their passwords, they often end up calling help desks or support centers, consuming valuable time. Password-reset inquiries account for up to 6% of call center activities, costing large organizations between $5 million and $20 million annually, according to McKinsey.[7]

Gartner estimates that these resets are even more frequent and costly, comprising 20% to 50% of all help desk calls.[8]

As long as service providers require passwords for authentication, weak security, frustrating customer experiences, and costly support requirements are inevitable.

Problems with SMS-based Two-Factor Authentication

To address some of the security shortcomings of passwords, some companies, websites, services, and applications have adopted SMS-based two-factor authentication (2FA). This type of authentication requires users to use SMS to provide a second factor of authentication in addition to a password. For example, an SMS message with a numerical string is sent to a mobile phone associated with the user's account. By entering the string, the user is demonstrating that, in addition to knowing the password for accessing the account, the user has control over a mobile device associated with the account.

That works in theory, but in practice SMS-based two-factor authentication has been shown to be vulnerable to hijacking, enabling attackers who have discovered users' passwords to intercept the transmitted numerical strings and masquerade as the owners of the mobile devices.[9]

Another problem is that SMS messages sometimes fail to arrive, or that the user is trying to login but she has no service or is out of power. In these cases, the user must find some other way, if possible, of providing a second factor for authentication.

Another serious problem is man-in-the-middle attacks that interpose themselves between users and the websites they're trying to reach, and trick users into entering usernames, passwords, mobile numbers, and SMS codes sent to those mobile numbers. By the time the attack is complete, the attackers have gleaned login credentials and an SMS code that can be used to access the legitimate site the user was trying to reach. Nearly all traditional strong authentication mechanisms, including mobile push authenticators, are vulnerable to these attacks.

WebAuthn Use Cases

WebAuthn makes rapid and easy web authentication a reality for users. Let's take a look at a few ways the new standard can be used to streamline login to a website, service, or application.

WebAuthn User Registration

A user wants to create an account for her online service provider. Instead of entering a username and password, she simply enters a username. In response, the online service provider that supports WebAuthn authentication asks her to register an authentication credential that will be associated with her account.

[7] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience

[8] https://www.infosecurity-magazine.com/webinars/password-management-getting/

[9] https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin

Thanks to the flexibility of WebAuthn, the user can choose whichever authentication method she likes, as long as it is supported by her device. For example, if she's working on a Windows 10 PC, she has the option of entering a credential with:

An internal authenticator, which accepts inputs such as:

- A PIN
- A facial scan
- A fingerprint scan
- A passphrase spoken aloud and validated by voice recognition software

An external authenticator, such as:

- A hardware security key

Support for internal authenticators varies from device to device. To support internal authenticators, a device must include a special security chip known as a Trusted Platform Module (TPM) to handle public and private keys.[10] Most recent business-grade laptops, desktops, and smartphones include these special chips. Devices must also include whatever cameras or biometric readers are required for the types of input being supported; for example, a device requires a fingerprint reader to support fingerprint scans.

The customer in our example chooses to use a hardware security key as her authentication option. Once she inserts the security key and taps to authenticate herself, her WebAuthn-compliant browser sends her account information and authentication credential back to the online service provider, which creates her account and binds her authentication credential with her account. The next time she logs in, she can quickly and easily authenticate without needing to enter a password.

And that's it. In less than a minute, she has created a secure account for an online service provider. Now she can quickly and securely authenticate any time she likes.

- She has created a secure login credential.
- She doesn't have a new password that she has to memorize.
- She hasn't had to go through the insecure and cumbersome process of SMS text message verification.

She simply registered herself using her preferred authentication method.

Note that for optimal security and control, the best practice is always to use a hardware security key as the first authentication option when registering a new account, since hardware security keys are independent of laptops, tablets, and other devices, and can be used to bootstrap a new device if an old device ever needs to be replaced.

Passwordless User Authentication

When a user wants to log in to her online service provider going forward, she simply enters her username. The online service provider will then prompt the user to take some physical action to authenticate herself, thereby assuring that the login request is coming from a person, rather than a malicious script.

The user authenticates using any one of the authentication methods she has already registered including:

An internal authenticator that supports:

- Entering a PIN
- Using a fingerprint scan
- Using a facial scan
- Using voice recognition

Inserting and tapping a hardware security key

Once the user authenticates, the online service provider immediately logs her in.

[10] https://trustedcomputinggroup.org/work-groups/trusted-platform-module/

Establishing a Portable Root of Trust

The WebAuthn standard supports two types of authenticators: internal authenticators, such as a fingerprint scanner built into a smartphone, and external authenticators, such as a hardware security key that can be used with a laptop, or mobile device. The external authenticators offer an additional advantage: Users can use them to establish a portable "root of trust."

A root of trust is a secure, irrefutable source for verifying the user's identity and for delegating trust to specific devices, such as smartphones, tablets, laptops, and desktops, under the user's control.

By placing this trust in an external authenticator, a user gains the ability to authorize other devices easily, as needed. Internal authenticators offer convenience but are limited to authenticating a user from a specific device. Should that device be lost or become corrupted, the user can use the external authenticator either to:

- re-authenticate the device
- authorize a replacement device and instantly gain access to all their accounts without having to reset passwords and receive dozens of SMS messages

The best practice for WebAuthn authentication is to register two external authenticators for each website, service, or application, to ensure continuous access even if one of their authenticators is lost.

Conclusion

The WebAuthn standard opens the door to a new, streamlined, and more secure user web experience, in which securely logging into websites, services, and apps takes just seconds from any device.

At the same time, WebAuthn closes the door on the poor user experience, security vulnerabilities, and financial risk of the password era. Data breaches caused by leaked or stolen passwords have cost organizations billions of dollars in the past few years. WebAuthn promises to reduce these breaches and curtail these costs.

Users can now expect new options for strong authentication that take advantage of both external security keys and authenticators built-in to devices.

Web development teams, as well as security and IT teams responsible for Identity and Access Management and security in their own organizations, should begin looking for products that support the WebAuthn standard, so that public sector employees, contractors, partners and customers can benefit from improved security and usability. At the same time, development teams for websites, services, and apps should begin working with the WebAuthn specification, so that they can build support for WebAuthn into their upcoming software releases and offer WebAuthn-supported authentication to users.

Already supported natively by all major browsers and most platforms, WebAuthn is poised to become ubiquitous in online life. By adopting this standard, organizations can – at last – make authentication truly secure and easy for users.

How to Get Started with WebAuthn

If you'd like to learn more and even get some hands-on experience with WebAuthn, here are some free resources you can turn to.

- Read an overview of WebAuthn on the Yubico website: www.yubico.com/webauthn
- Read the other white papers in the Yubico WebAuthn series:
  - *The WebAuthn Standard - Why it Matters and How it Works*
  - *Establishing a Secure Portable Root of Trust with WebAuthn*
  - *SIM Swap: Protecting against Account Takeovers with WebAuthn*
- Try out the Yubico WebAuthn demo site: demo.yubico.com/webauthn
- Visit the Yubico developer site and access free developer resources for WebAuthn: developer.yubico.com/webauthn
- Read the complete WebAuthn specification on the W3C site: https://www.w3.org/TR/webauthn/

> "Now is the time for web services and businesses to adopt WebAuthn to move beyond vulnerable passwords and help web users improve the security of their online experiences. W3C's Recommendation establishes web-wide interoperability guidance, setting consistent expectations for web users and the sites they visit. W3C is working to implement this best practice on its own site."
>
> —Jeff Jaffe, CEO, W3C

yubico

About Yubico

Yubico sets new global standards for simple and secure access to computers, mobile devices, servers, and internet accounts.

The company's core invention, the YubiKey, delivers strong hardware protection, with a simple touch, across any number of IT systems and online services. The YubiHSM, Yubico's ultra-portable hardware security module, protects sensitive data stored in servers.

Yubico is a leading contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor open authentication standards, and the company's technology is deployed and loved by 9 of the top 10 internet brands and by millions of users in 160 countries.

Founded in 2007, Yubico is privately held, with offices in Sweden, UK, Germany, USA, Australia, and Singapore. For more information: www.yubico.com.