yubico

WEBAUTHN WHITE PAPER SERIES SEPTEMBER 2019

Establishing a Secure Portable Root of Trust with WebAuthn

Executive Summary

This paper is the third in a series of WebAuthn whitepapers published by Yubico. For an introduction to WebAuthn and why it is both more secure and easier to use, read, *Introducing WebAuthn: Enabling a Streamlined and More Secure User Authentication Experience.* For a deeper dive into the problems with passwords, how WebAuthn addresses them, and how to implement WebAuthn support from a developer perspective, read the second paper, *The WebAuthn Standard – Why it Matters and How it Works.*

Nearly every website, service, or application today relies on passwords. But passwords are cumbersome and problematic since they're prone to being intercepted, guessed, and hacked. Today stolen passwords play a key role in the majority of data breaches.

WebAuthn, a new web standard adopted by the World Wide Web Consortium (W3C), enables websites, services, and applications to easily deploy strong authentication without relying on weak passwords. With native support in all major platforms and browsers, WebAuthn offers users expanded choices for authenticating. They can use an external authenticator, such as a hardware security key, to respond to an authentication request and verify their identity over the internet. Or they can use an internal authenticator built into the platform. Either way, a biometric or PIN can be used to verify the user's authentication.

While these authenticators offer the best available protection, especially against phishing attacks targeting account takeovers, an important consideration is how to establish a "root of trust." This is the mechanism by which a user recovers an account or establishes their identity on a new device. Historically this has mostly been accomplished by the use of some other authentication method, e.g. username/password, SMS, or email. However, all of these introduce a "weak link" which can then be exploited by an attacker.

With WebAuthn, users now have the ability to establish an external authenticator as a portable root of trust, offering benefits for establishing trust on new and replacement computing devices. Establishing a portable root of trust offers users important benefits for data security and convenience:

- Optimal security when onboarding a new device
- Account recovery after device loss, theft, or compromise
- Convenient authentication for high-risk or high-value transactions
- Convenient access across all of a user's devices
- Uninterrupted access even when internet access is interrupted
- Authentication in environments with restricted mobile access
- Integration with legacy systems

For WebAuthn-supported websites, services, and applications, the best practice is to use an external authenticator such as a hardware security key when setting up accounts and to keep a backup external authenticator in case the first one is ever lost or damaged.

Introduction

Everyone is tired of passwords.

Users are tired of having to remember them, to type them, and to change them every few months on websites with strict password-rotation rules.

IT security teams are tired of trying to protect passwords, which too often end up being stolen or guessed anyway. Once stolen, passwords are often used to perpetuate further security attacks. Stolen passwords are involved in 81% of data breaches, and each of those breaches costs $3.9 million on average.[1]

Support centers and help desks are tired of fielding emails and calls from users requesting that their passwords be reset. And IT organizations are tired of the high support costs these password resets incur.

Passwords are too cumbersome, too insecure, too time-consuming, and too costly. Fortunately, there's now a better way of securely authenticating users.

In March 2019, the World Wide Web Consortium (W3C), the primary standards body for the Web, ratified the specification for WebAuthn, a new standard that simplifies and strengthens authentication for websites, services, and applications.[2]

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 are committed to supporting the WebAuthn standard.

Why WebAuthn Matters

For any website, service, or application that requires users to authenticate, the WebAuthn standard is important for several reasons:

- **Standardization**
  The approval of WebAuthn by the W3C enables the standardization of 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 exasperating hassles of passwords (and SMS codes) 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 using a built-in authenticator or 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 costs such as productivity costs, support costs, and financial penalties accruing from data breaches perpetrated by attackers using stolen or guessed passwords.
- **Accelerated Software Development**
  WebAuthn accelerates software development by enabling developers to implement best-in-class registration and authentication services with just two commands.

This new standard brings a higher level of secure authentication to all users on the web.

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

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

Considerations for the New Passwordless World

Thanks to WebAuthn, we are now entering a new world of passwordless authentication. This new world has broad implications for how users interact with all their computing devices.

Consider the password-based online world we all live in now. Most users work with multiple devices, if not in the course of a day then certainly in the course of a week. These devices include smartphones, tablets, laptops, and desktops. Users often have to manually install the same apps on each device, and then log in individually to each app. In addition, they usually access the same cloud apps from multiple devices and may cache their app passwords on each device.

If a password is compromised, users may have to change the password and reset caches (their "saved passwords") on multiple devices. If a device is lost or stolen, users have to re-enter passwords on the replacement device. To be cautious, though, they might want to change all the passwords associated with apps installed on or accessed from any lost or stolen device.

In this new passwordless world enabled by WebAuthn, it's possible to have a portable root of trust, such as a hardware security key, that manages cryptographic keys for all accounts for all apps for all devices. The portable root of trust works on every device a user has. And enabled by the new WebAuthn standard, it always works the same way. The portable root of trust enables users to move from device to device at any time, accessing accounts without ever having to set up, remember, type, or change a password.

If a user gets a new device, she can use the hardware security key to "bootstrap" or transfer trust to the new device, so that the device can be used to access the passwordless accounts the user is interested in.

In this new passwordless model, authentication is easy (no password memorization required), and it's portable, capable of being transferred to any device whenever or wherever the user needs it. Wherever the user is, trust is there, in the form of an easy to use hardware security key.

Creating a Portable Root of Trust with Hardware Security Keys

Besides simplifying web authentication and making it more secure, WebAuthn makes it possible for users to take advantage of a new model for trust. Specifically, it enables a user to maintain an external authenticator, such as a hardware security key, that stores all the credentials a user needs to securely authenticate.

When a hardware security key connects to a smartphone, tablet, laptop, or desktop, it can assure a website, service, or application that the user and the device are associated with a known account. It can also be used to bootstrap trust for the new device, so that in the future the user can login from that device using built-in authenticators, such as fingerprint and facial scanners, without requiring the hardware security key.

The hardware security key becomes the root of trust—the basis of a user's identity and authority for accessing accounts over the web or for delegating trust to another device, such as the user's laptop. Rather than having credentials scattered across the password databases of countless websites, a user is in full control of her credentials, which can be granted or revoked as she wishes, without the risk of account takeover from a website, service, or application.

Hardware security keys supporting WebAuthn standard use public key cryptography and generate and store authentication secrets in a secure, tamper-resistant hardware element. The secure element contains no personally identifiable identity data, so an ill-intentioned person finding an external authenticator in a café, for example, will have no idea which sites and accounts the authenticator is associated with.

The Benefits of a Hardware Security Key as a Portable Root of Trust

To take full advantage of WebAuthn, users should use hardware security keys as their root of trust. There are numerous benefits to having a hardware security key as a portable, phishing-resistant root of trust.

- **Optimal Security and User Experience When Onboarding a New Device**
  To authenticate to a service from a new device, the user needs to present some type of portable credential. Traditionally users would use passwords, SMS messages, or QR codes, but all those methods are cumbersome and insecure. A better solution is to set up a hardware security key as an external authenticator and optionally use that security key to "bootstrap" the internal authenticator, if one exists. The security key vouches for the user to the internal authenticator.

Once bootstrapped, the internal authenticator can vouch for the user. In this way, a security key can serve as a portable root of trust for all the devices–smartphones, tablets, laptops, and desktops–belonging to the user and for all WebAuthn-compliant services with whom the user has accounts.

- **Account Recovery after Device Loss, Theft, or Compromise**
  If a user loses a device with an internal authenticator, the user can use the security key to register a new device for access. Registration is fast and easy: The user simply logs into the site from the new device, then taps or inserts the security key to login. Once logged in, the new device can be registered with the resource. There's no need for calls to a help desk or support line for temporary passwords, password resets, or SMS codes. The process takes a matter of minutes.
- **High-risk or High-value Transactions or Applications**
  The security key can be used for an additional level of assurance on any trusted device any time a user needs to "step up authentication" as part of authorizing a high-risk or high-value transaction, such as a large money transfer.
- **Convenient Access Across All of a User's Devices**
  Today's hardware security keys are small and lightweight (about the size of a standard USB stick or even smaller) and can be carried everywhere the user needs to go. They are available for authenticating even on devices the user does not own.
- **Uninterrupted Access**
  Security keys are available with varying degrees of physical protection, and Yubico keys in particular are designed to be highly durable, crush- and water-resistant, and continuously available. Because they do not require batteries, they never lose their charge. They are available whenever users need them.
- **Authentication in Environments with Restricted Mobile Access**
  There are many areas where mobile phones are not allowed, including call centers, manufacturing sites, healthcare facilities, and other secure locations. A security key provides a portable solution for authentication without requiring the user to carry a smartphone in these locations.
- **Integration with Legacy Systems**
  Some legacy systems do not support newer standards such as WebAuthn, but might support older authentication standards such as OTP or SmartCard whose credentials can be stored in the secure chip on a security key. Security keys are available that support both new WebAuthn

credentials as well as older types of credentials in a single, convenient, and portable format.

Best Practices for Using External Authenticators

Here are some best practices for using external authenticators.

- Users should use an external authenticator such as a hardware security key when creating initial user credentials for any WebAuthn-supported website, service, or app. Once credentials have been created with a hardware security key, users can add other credentials with an internal authenticator.
- If an external authenticator is left connected to a computer, it is always best to set up a second factor for accessing a website, service, or application. The WebAuthn standard accepts second factors such as PINs, facial scans, and fingerprint scans, depending on the capabilities of the authenticator. A second-factor ensures that only the rightful owner is using the authenticator.
- Users should use a back-up authenticator when setting up accounts for critical websites, services, and applications. If one authenticator is lost or stolen, the second one can be used as a replacement. When an account is accessed using the second authenticator, account-management tools can be used to disable access from the lost or stolen authenticator.
- IT organizations should issue external authenticators to all employees and trusted contractors, so that they can securely access their accounts without any risk of passwords being lost, stolen, or phished.
- Developers of services and applications should require an external authenticator for high-value transactions such as money transfers, as well as to re-validate user credentials once a month.

Conclusion

WebAuthn gives users control over their credentials for websites, services, and applications, and lets them choose how they authenticate from their devices. It also eliminates the problem of leaked passwords leading to costly data breaches. Already adopted by all major web browsers and platforms, WebAuthn provides the data security and ease of use that have been missing from password-based authentication.

Designating a hardware security key as a portable root of trust gives users the ultimate control over their login credentials and devices, and enables organizations to improve data security and login experiences at scale. Portable and easy-to-use, hardware security keys ensure that account access is always available and secure, even when laptops or other devices are lost, stolen, or compromised. Using a hardware security key as a portable root of trust enables users to realize the full benefits of the WebAuthn standard.

How to Get Started Establishing a Root of Trust

If you'd like to learn more about root of trust and WebAuthn, here are some free resources.

- Learn about the YubiKey hardware security key on the Yubico website: https://www.yubico.com/products/yubikey-hardware/
- Read an overview of Root of Trust on the Yubico website: https://www.yubico.com/root-of-trust/
- Read an overview of WebAuthn on the Yubico website: https://www.yubico.com/solutions/webauthn/
- Read the other white papers in the Yubico WebAuthn series:
  - *Introducing WebAuthn: Enabling a Streamlined and More Secure User Authentication Experience*
  - *The WebAuthn Standard - Why it Matters and How it Works*
  - *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: https://developers.yubico.com/WebAuthn/
- Read the complete WebAuthn specification on the W3C site: https://www.w3.org/TR/webauthn/

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.