FIDO2: A WEB WITHOUT PASSWORDS

W3C TRACK AT THE WEB CONFERENCE

Andrew Shikiar
Chief Marketing Officer
FIDO Alliance

May 15, 2019
THE WORLD HAS A PASSWORD PROBLEM
CONSUMERS HAVE A PASSWORD PROBLEM

90+ ACCOUNTS

Per average user (Oxford University)

<5 PASSWORDS

Per user, and 50% haven’t changed said password in last 5 years (Pew)

55%

Of IT leaders re-use a single password (Sailpoint)

1,300 YEARS

Collectively spent by humans each day entering passwords (Microsoft)

CLUMSY | HARD TO REMEMBER | NEED TO BE CHANGED ALL THE TIME
BUSINESSES HAVE A PASSWORD PROBLEM

81%
Data breaches that involved weak, default, or stolen passwords (VDBR 2016)

36%
Rise in phishing attacks in 2018 (Webroot)

1,244
Breaches in 2018, with a 126% jump in exposed records containing PII (ITRC)

$1M
Annual cost to a large corporation for password resets (Forrester)

20-50%
Of helpdesk calls are for password resets (at $70/reset) (Gartner/Forrester)

49%
Password-driven cart abandonment rate (Visa)
ONE-TIME PASSCODES

Improve security but aren’t easy enough to use

- SMS Reliability
- Token Necklace
- User Confusion
- Still Phishable
INDUSTRY IMPERATIVE: SIMPLER AND STRONGER

Open standards for simpler, stronger authentication using public key cryptography
FIDO Alliance is the global industry collaboration dedicated to solving the password problem

...with no dependency on “shared secrets”
LEADING THE EFFORT

CONSUMER ELECTRONICS
Google
Microsoft
Lenovo
int
docomo
infineon
Samsung
Qualcomm
arm
NXP

SECURITY & BIOMETRICS
Synaptics
Thales
Feitian
RSA
Daon
IDEMIA
Raon
HPR
eWBM
Onfido
Nok
VMware
OneSpan

HIGH-ASSURANCE SERVICES
Aetna
LINE
Visa
Amazon
Facebook
PayPal
Alibaba.com
American Express
Bank of America
Mastercard
Wells Fargo
ING
USAA
BCcard
Yahoo!

All Rights Reserved | FIDO Alliance | Copyright 2019
INDUSTRY PARTNERSHIPS
HOW FIDO WORKS
OLD AUTHENTICATION WITH PASSWORDS

1. Password could be stolen from the server

2. Password might be entered into untrusted App / Website ("phishing")

3. Too many passwords to remember (>re-use / cart Abandonment)

4. Inconvenient to type password on phone
HOW DOES FIDO WORK?

User verification → Authenticator Device → FIDO Authentication
FIDO AUTHENTICATORS

We see “Bound” or “Platform” Authenticators, (authenticators that are an integral part of a smartphone or laptop)

We see “Roaming” Authenticators, (authenticators that can be connected to different smartphones/laptops using CTAP)

In both categories you find support for different modalities

User Presence Challenge (“A” user)

User Verification Methods (“THE” user)
HOW DOES FIDO WORK? - REGISTRATION

1. **Invitation to Register**
   - User approval is required before private keys can be created.
   - The Authenticator verifies the user's identity.
   - Public/private keypair is created.
   - Signed Attestation Object is generated.
   - Public key is registered with the account.

2. **Public Key**
   - Registered with the account.

3. **FIDO Registration**
   - Invites the user to register.

4. **Require user gesture before private keys can be created**

All Rights Reserved | FIDO Alliance | Copyright 2019
HOW DOES FIDO WORK? - AUTHENTICATION

Authenticator

Require user gesture before private key can be used

Private key dedicated to one app

Challenge

(Signed) Response

FIDO Authentication

Public key
FIDO AUTHENTICATION VS. PASSWORDS

1. No secrets stored on the server

2. Authenticator cannot be “tricked” by phishing

3. Nothing to remember, no friction added to transaction process

4. Single gesture convenience for User

Authenticate

FIDO Authentication

Challenge

(Signed) Response

Public key

Private key
dedicated to one app

Require user gesture before private key can be used

User verification
FIDO USER EXPERIENCES

Passwordless Experience

1. Authentication Challenge
2. Biometric User Verification*
3. Authenticated Online

Second Factor Experience

1. Second Factor Challenge
2. Insert Security Key* / Press Button
3. Authenticated Online

*There are other types of authenticators
FIDO Specifications

FIDO UAF
FIDO U2F
(@FIDO)

CTAP
(@FIDO)

WebAuthn
(@W3C)

FIDO2
BACKED BY CERTIFICATION (>500)

• Functional Certification (End-to-End):
  • Conformance Testing
  • Interoperability Testing

• Authenticator Security Certification Levels
  • How well do you protect the private key?
  • 3rd-party laboratory verification
  • Complemented by Biometric Component certification

• Universal Server:
  • Ensures compatibility with all FIDO Certified Authenticators
FIDO IN THE MARKET
FIDO NOW A W3C WEB STANDARD

FIDO2 (CTAP & W3C Web Authentication)

FIDO2 BRINGS STRONGER, SIMPLER AUTHENTICATION TO INTERNET USERS WORLDWIDE
FIDO IS AN ITU STANDARD

x.1277 -- ITU ratification of FIDO UAF
x.1278 -- ITU ratification of FIDO2 CTAP (includes CTAP1/U2F)
BIOMETRIC CERTIFICATION

Samsung Galaxy S10 and S10+

First to Achieve FIDO Biometric Certification

All Rights Reserved | FIDO Alliance | Copyright 2019
MOBILE APPS AND WEBSITES CAN NOW LEVERAGE FIDO STANDARDS TO PROVIDE A SIMPLER AND SECURE BIOMETRIC LOGIN FOR USERS ON OVER A BILLION DEVICES SUPPORTING ANDROID 7.0 OR LATER
Over **800 million users** with Microsoft accounts can now leverage built-in biometrics or local PINs to access their desktops and related Microsoft services.
CROSS PLATFORM SUPPORT
“Firefox 66 supports using the Windows Hello feature for Web Authentication on Windows 10, enabling a passwordless experience on the web that is hassle-free and more secure.

“Firefox has supported Web Authentication for all desktop platforms since version 60, but Windows 10 marks our first platform to support the new FIDO2 “passwordless” capabilities for Web Authentication.”
Special Thanks to Adam Powers & Akshay Kumar

Note: “Android” means “via Google Play Services”
FIDO CERTIFIED ECOSYSTEM (SAMPLE)

SONY  LG  SAMSUNG  FUJITSU  SHARP  Samsung

Lenovo  Intel  Android  Android

SECURITY KEYS (and more)

HANDSETS + PCS

Google  Microsoft  Daon  RSA

FEITIAN  OneSpan  nok

ING  eBay  LINE

CLOUD/SERVER SOLUTIONS
FIDO IS BEING USED AROUND THE WORLD
(Sample of deployments in production)
SECURE BY DESIGN

Based on public key cryptography

Keys stay on device

No server-side shared secrets

Biometrics, if used, never leave device

No 3rd party in the protocol

No link-ability between services or accounts
SECURE IN PRACTICE

85,000 employees over 18 months

No ATO’s from phishing since using FIDO

Google: Security Keys Neutralized Employee Phishing

Google has not had any of its 85,000+ employees successfully phished on their work-related accounts since early 2017, when it began requiring all employees to use physical Security Keys in place of passwords and one-time codes, the company told KrebsOnSecurity.

Security Keys are inexpensive USB-based devices that offer an alternative approach to two-factor authentication (2FA), which requires the user to log in to a Web site using something they know (the password) and something they have (e.g., a mobile device).

A Google spokesperson said Security Keys now form the basis of all account access at Google.

“We have had no reported or confirmed account takeovers since implementing security keys at Google,” the spokesperson said. “Users might be...
WHAT’S NEXT...

KNOW YOUR CUSTOMER (eKYC/ID&V)

IoT Device ID/AuthN
FIDO Authentication is the industry’s response to the password problem

- **INDUSTRY SUPPORT** - FIDO represents the efforts of some of the world’s largest companies whose very businesses rely upon better user authentication

- **THOUSANDS OF SPEC DEVELOPMENT HOURS** - Now being realized in products being used every day

- **ONGOING INNOVATION** - Specifications, certification programs, and deployment working groups establishing best implementation practices

- **ENABLEMENT** - Leading service providers representing billions of user identities are already FIDO-enabling their authentication processes
Take Part in the FIDO Ecosystem

- Build FIDO Certified Solutions
- Deploy FIDO Authentication
- Join the Alliance
- Attend FIDO Events

Email: info@fidoalliance.org
Twitter: @fidoalliance
www.fidoalliance.org