FIDO: Open Standards for Digital Authentication

ReBIT - Securing Digital Payments Webinar
May 27, 2021

David Turner
Director of Standards Development
david@fidoalliance.org
Introduction
Industry imperative: Simpler and stronger

Open standards for simpler, stronger authentication using **public key cryptography**

Single Gesture Possession-based Authentication
Classifying threats

Physical attacks possible on lost or stolen devices (3% in the US in 2013)

- Physically attacking user devices
  - steal data for impersonation
- Physically attacking user devices
  - misuse them for impersonation

Scalable attacks

- Remotely attacking lots of user devices
  - steal data for impersonation
- Remotely attacking lots of user devices
  - misuse them for impersonation
- Remotely attacking lots of user devices
  - misuse authenticated sessions
- Remotely attacking central servers
  - steal data for impersonation
Authentication with FIDO2
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

User verification

Device

Internet

Authentication
Modern authentication with FIDO
Modern authentication with FIDO

User verification

Authenticator

Require user gesture before private key can be used

Private key dedicated to one app

Challenge

(Signed) Response

FIDO Authentication

Public key
Modern authentication with FIDO

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

User verification

Require user gesture before private key can be used

Private key (handle) per account

Challenge

(Signed) Response

Public key

FIDO Authentication
The FIDO Authenticator

User verification

Authenticator

FIDO Authentication
Client-side biometrics

Trusted Execution Environment (TEE)

FIDO Authenticator as Trusted Application (TA)

User Verification / Presence

Store at Enrollment

Compare at Authentication

Unlock after comparison

Attestation Key

Authentication Key(s)
FIDO authenticators

We see “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)
Cross-platform deployment capabilities
In summary: Stronger

- 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
In summary: Simpler

- Reduces reliance on complex passwords
- Single gesture to log on
- Works with commonly used devices
- Same authentication on multiple devices
- Fast and convenient
Thank you!

@FIDOALLIANCE
WWW.FIDOALLIANCE.ORG

David Turner
david@fidoalliance.org