FIDO & You

How FIDO Standards Enhance Security & Protect Against Threats

Paul Grassi
Senior Standards and Technology Advisor
National Strategy for Trusted Identities in Cyberspace (NSTIC)
National Program Office
NIST
AGENDA

The Problem
The Solution
The Alliance
Updates
Data Breaches...

780 data breaches in 2014

>1 billion records since 2012

$3.5 million cost/breach
“76% of 2012 network intrusions exploited weak or stolen credentials”

*2013 Data Breach Investigations Report*
The world has a **PASSWORD PROBLEM**
ONE-TIME PASSCODES
Improve security but aren’t easy enough to use

- SMS Reliability
- Token Necklace
- User Confusion
- Still Phishable
WE NEED A NEW MODEL
WE CALL OUR NEW MODEL Fast IDentity Online

online authentication using public key cryptography
AGENDA

The Problem

The Solution

The Alliance

Updates
THE OLD PARADIGM

SECURITY

USABILITY
THE FIDO PARADIGM

SECURITY

Strong

Weak

USABILITY

Easy

Poor
HOW OLD AUTHN WORKS

The user authenticates themselves online by presenting a human-readable secret
HOW FIDO AUTHN WORKS

The user authenticates “locally” to their device by various means

The device authenticates the user online using public key cryptography
ONLINE AUTHENTICATION USING PUBLIC KEY CRYPTOGRAPHY
Passwordless Experience (UAF Standards)

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

Second Factor Experience (U2F Standards)

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

*There are other types of authenticators
FIDO Registration

1. Invitation Sent
User is in a Session
Or
New Account Flow

2. User Approval

3. New Keys Created

4. Registration Complete

Pubic Key Registered
With Online Server
FIDO Authentication

1. User needs to login or authorize a transaction

2. FIDO Challenge

3. Key Selected & Signs

4. User Approval

Login Complete

Signed Response verified using Public Key Cryptography
FIDO UAF
UNIVERSAL AUTHENTICATION FRAMEWORK

Same User as enrolled before?

Same Authenticator as registered before?

AUTHENTICATOR
THE BUILDING BLOCKS

FIDO USER DEVICE

- BROWSER/APP
- FIDO CLIENT
- ASM
- FIDO AUTHENTICATOR
  - Authentication Private Keys
  - Attestation Private Keys

RELYING PARTY

- WEB SERVER
  - TLS Server Key
- FIDO SERVER
  - FIDO
  - UPDATE
    - Cryptographic Authentication Public Keys DB
    - Authenticator Metadata & Attestation Trust Store

Confidential
ATTESTATION & METADATA

FIDO Authenticator

Signed Attestation Object

FIDO Server

Verify Trust Anchor (Available from Metadata Service or Other Source)

Metadata

Understand Authenticator Characteristic (Using Info From Metadata or Other Source)
STEP 1

UAF AUTHENTICATION
DEMO EXAMPLE
STEP 2
UAF AUTHENTICATION DEMO EXAMPLE
STEP 3
UAF AUTHENTICATION DEMO EXAMPLE
STEP 4

UAF AUTHENTICATION DEMO EXAMPLE
FIDO U2F
UNIVERSAL 2ND FACTOR

Is a user present?

USER VERIFICATION

FIDO AUTHENTICATION

AUTHENTICATOR

Same authenticator as registered before?

Confidential
All Rights Reserved. FIDO Alliance. Copyright 2016.
Step 1
U2F AUTHENTICATION DEMO EXAMPLE
Step 2

U2F AUTHENTICATION DEMO EXAMPLE
Step 3

U2F AUTHENTICATION DEMO EXAMPLE
Step 4
U2F AUTHENTICATION DEMO EXAMPLE
USABILITY, SECURITY
and
PRIVACY
No 3rd Party in the Protocol

No Secrets on the Server Side

Biometric Data (if used) Never Leaves Device

No Link-ability Between Services

No Link-ability Between Accounts
Better security for **online services**
Reduced cost for the **enterprise**
Simpler and safer for **consumers**
AGENDA

The Problem
The Solution
The Alliance
Updates
The FIDO Alliance is an open industry association of over 250 global member organizations.
Physical-to-digital identity

User Management

Federation

Single Sign-On

Authentication

MODERN AUTHENTICATION

Passwords

Strong

Risk-Based
FIDO Alliance Mission

1. Develop Specifications
2. Operate Adoption Programs
3. Pursue Formal Standardization
Board Members
Government Members

“The fact that FIDO has now welcomed government participation is a logical and exciting step toward further advancement of the Identity Ecosystem; we look forward to continued progress.”

-- Mike Garcia, NSTIC NPO
Our mission is highly complementary to many other associations around the world. We welcome the opportunity to collaborate with this growing list of industry partner organizations.
FIDO TIMELINE

- **Alliance Announced**: FEB 2013
- **FIDO Ready Program**: DEC 2013
- **Specification Review Draft**: FEB 2014
- **First Deployments**: FEB-OCT 2014
- **FIDO 1.0 FINAL**: DEC 9 2014
- **Certification Program**: MAY 2015
- **New U2F Transports**: JUNE 2015
- **Broad Adoption**: TODAY >250 Members

6 Members

Confidential
2014 FIDO ADOPTION

“PayPal and Samsung Enable Consumer Payments with Fingerprint Authentication on New Samsung Galaxy S5”
Feb 24, 2014

“Secure Consumer Payments Enabled for Alipay Customers with Easy-to-Use Fingerprint Sensors on Recently-Launched Samsung Galaxy S5”
September 17, 2014

“Google Launches Security Key, World’s First Deployment of Fast Identity Online Universal Second Factor (FIDO U2F) Authentication”
October 21, 2014
2015 FIDO ADOPTION

“Microsoft Announces FIDO Support Coming to Windows 10”  
Feb 23, 2015

“Google for Work announced Enterprise admin support for FIDO® U2F ‘Security Key’”  
April 21, 2015

“Qualcomm launches Snapdragon fingerprint scanning technology”  
March 2, 2015

“Microsoft Announces FIDO Support Coming to Windows 10”  
Feb 23, 2015

“Largest mobile network in Japan becomes first wireless carrier to enhance customer experience with natural, simple and strong ways to authenticate to DOCOMO’s services using FIDO standards.”  
May 26, 2015

“Today, we’re adding Universal 2nd Factor (U2F) security keys as an additional method for two-step verification, giving you stronger authentication protection.”  
August 12, 2015

“[T]he technology supporting fingerprint sign-in was built according to FIDO (Fast IDentity Online) standards.”  
September 15, 2015

“GitHub says it will now handle what is called the FIDO Universal 2nd Factor, or U2F, specification.”  
October 1, 2015
Deployments are enabled by **FIDO Certified™ products** available today
Available to anyone
Ensures interoperability
Promotes the FIDO ecosystem

Steps to certification:
1. Conformance Self-Validation
2. Interoperability Testing
3. Certification Request
4. Trademark License (optional)

fidoalliance.org/certification
FIDO 2.0 Technology Working Group
The mission of the new FIDO 2.0 Specification Technology Working Group is to consider future requirements, and to ensure widespread platform support within the authentication ecosystem among devices, clients, and servers.
FIDO 2.0 & W3C

November 2015

FIDO Authentication Poised for Continued Growth as Alliance Submits FIDO 2.0 Web API to W3C

• W3C has accepted our submission
• Specifications required to define a FIDO-compliant Web API
• Designed to extend FIDO’s existing reach to all platforms
• OEM community should begin to plan their support now
• RP community should deploy FIDO 1.x now knowing FIDO standards are “future proof” -- strategically positioned as the de facto authentication scheme for the Web & OS Platforms

February 2016

W3C Launches New Standards Effort Based on FIDO 2.0 Web APIs

• W3C announces the chartering of the Web Authentication Working Group
• Standardizing the submitted FIDO Web APIs can ensure standards-based strong authentication across all Web browsers and related Web platform infrastructure
• The first meeting of the Working group was early March
FIDO Alliance Mission

2. Operate Adoption Programs

FIDO Certification™ Program
Adding “security certification program” and exploring possible biometrics program

FIDO UAF Metadata Service
Launch of the UAF Metadata Service; will be adding Attestation Service for U2F

FIDO Alliance Liaison Program
Launched new program to foster collaboration, expecting organic growth

FIDO Marketing & Education Programs
More webinars, seminars, conference talks, and targeted outreach - esp. in APAC
FIDO Alliance Mission

Submit mature technical Specification(s) to recognized SDO’s...

- We will evaluate maturity for this purpose after more deployments
- We will use the Liaison Program to collaborate with SDO’s, e.g. W3C
- All other specifications for FIDO 1.x & 2.x remain in the Alliance today
WHY NIST CARES
Mission Alignment

Called for in President’s Cyberspace Policy Review (May 2009):
a “cybersecurity focused identity management vision and strategy...that addresses privacy and civil-liberties interests, leveraging privacy-enhancing technologies for the nation.”

**Guiding Principles**

*Identity Solutions will be:*

- Privacy-Enhancing and Voluntary
- Secure and Resilient
- Interoperable
- Cost-Effective and Easy To Use

NSTIC calls for an **Identity Ecosystem**, “an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities.”
Spectrum of Privacy Enhancing Use Cases

Anonymous

PHR Site
Track BP/Steps
Diet
Other Sensitive Tx

Anonymity Retained

Strong Credentials (but passwords may still have a place)

No Proofing

401(k) Site
Change Allocation
Buy/Sell
Other Sensitive Tx

Strong Proofing

Paul Grassi

401(k) Site
Change Allocation
Buy/Sell
Other Sensitive Tx

Anonymity Retained

Strong Credentials (but passwords may still have a place)

No Proofing

PHR Site
Track BP/Steps
Diet
Other Sensitive Tx

Anonymous
Possible Government Use Cases

M-05-24
JOIN THE FIDO ECOSYSTEM