“Identity Standards Updates – FIDO”

Brett McDowell, Executive Director, FIDO Alliance

brett@fidoalliance.org
Data Breaches...

- 783 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

Poor

Easy

™
HOW OLD AUTHN WORKS

The user authenticates themselves online by presenting a human-readable secret.
The user authenticates “locally” to their device by various means.

The device authenticates the user online using public key cryptography.

**HOW FIDO AUTHN WORKS**

**LOCAL**

**ONLINE**

**AUTHENTICATOR**
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. User is in a Session Or New Account Flow

2. Invitation Sent

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. User Approval

3. Key Selected & Signs

4. Signed Response verified using Public Key Cryptography

Login Complete
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
  - Cryptographic Authentication Public Keys DB
  - UPDATE
    - Authenticator Metadata & Attestation Trust Store
FIDO Server

**Signed Attestation Object**

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

**FIDO Authenticator**

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

**FIDO Server**

**Metadata**

ATTESTATION & METADATA
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 2\textsuperscript{ND} FACTOR

Is a user present?

Same user as enrolled before?

USER VERIFICATION

AUTHENTICATOR

FIDO AUTHENTICATION

Same authenticator as registered before?
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 Fast IDentity Online (FIDO) Alliance is an open industry association of over 220 global member organizations.
✓ Services/Networks
✓ Devices/Platforms
✓ Vendors/Enablers

Board Members

- Alibaba Group
- Bank of America
- DISCOVER
- ING
- MasterCard
- PayPal
- USAA
- VISA
- NTT docomo
- Google
- Microsoft
- Lenovo
- Samsung
- CrucialTec
- Daon
- egis Technology
- Intel
- ARM
- Nak Nak LABS
- NXP
- Oberthur Technologies
- Qualcomm
- RSA
- Synaptics
- yubico
FIDO Alliance Mission

1. Develop Specifications
2. Operate Adoption Programs
3. Pursue Formal Standardization
FIDO SCOPE

- Single Sign-On
- Federation
- Authentication
- User Management
- Physical-to-digital identity

Modern Authentication

- Passwords
- Strong
- Risk-Based
AGENDA

The Problem
The Solution
The Alliance
Updates
FIDO TIMELINE

- **FIDO 1.0 Final**
- **First Deployments**
- **FIDO 1.0 Certification Program**
- **Fido U2F Certified**
- **New U2F Transports**
- **Broad Adoption**

- **Alliance Announced**
- **FIDO Ready Program**
- **Specification Review Draft**

- **FEB 2013**
- **DEC 2013**
- **FEB 2014**
- **FEB-OCT 2014**
- **DEC 9 2014**
- **MAY 2015**
- **JUNE 2015**
- **TODAY >220 Members**

- **6 Members**
2014 FIDO ADOPTION


2015 FIDO ADOPTION

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

"Qualcomm launches Snapdragon fingerprint scanning technology"
March 2, 2015

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

"As part of the bank’s ongoing commitment to staying ahead of advancements in mobile device authentication, the technology supporting fingerprint sign-in was built according to FIDO (Fast IDentity Online) standards."
September 15, 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)

NEXT EVENT: October 5th (U2F)
fidoalliance.org/certification
FIDO Alliance Announces Government Membership Program – US and UK Government Agencies are First to Join

Government Agencies to Participate in Development of FIDO Standards for Universal Strong Authentication

“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.”
What’s Next?
FIDO Alliance Mission

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 interoperability within the authentication ecosystem among devices, clients, and servers.
FIDO Alliance Mission

Operate Adoption Programs

FIDO Certification™ Program
Investigating the need/feasibility of adding “security” and “biometrics” testing

FIDO UAF Metadata Service
Formal launch of the UAF Metadata Service following current “soft launch”

FIDO Alliance Liaison Program
Launched new program with streamlined process to foster collaboration

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 ongoing
JOIN THE FIDO ALLIANCE
EXPERIENCE SIMPLER, STRONGER AUTHENTICATION