Universal Second Factor

IAM Online
November 11, 2015 - 2 pm ET

Keith Hazelton, University of Wisconsin
Stina Ehrensvard, Yubico
Kevin Casey, Yubico
Universal 2\textsuperscript{nd} Factor

Simple, secure, open and scalable 2FA
On this call

Keith
Senior IT Architect
WISC.edu

Stina
CEO & Founder
Yubico

Kevin
Product Manager
Yubico
The Authentication Landscape

**HIGH SECURITY**
- FIDO U2F: High security with unmatched simplicity, low cost and scalability

**SIMPLICITY & LOW COST**
- Consumer Biometrics
- Software auth apps

**COMPLEXITY & HIGH COST**
- Industrial Biometrics
- Security chips in phones/computers

**LOW SECURITY**
- Username Password
- Hardware OTP tokens
- Smart card
UW-Madison Requirements

Implement Stronger Authentication to Reduce Risk

- First, for 3,000 HR staff who work with restricted data
- Increasing concern over online activities of all campus parties
- Need solution to scale up by factor of 100
UW-Madison Requirements

Implement Stronger Authentication to Reduce Risk

- Our WebSSO is Shibboleth, so solution must integrate with IdP
- Some federated SPs expected to demand higher levels of assurance
- Address the persistent, evolving threat of phishing
- To achieve high levels of adoption, the solution must be
  - Convenient
  - Low cost
U2F Hardware Tokens

Two factors. One touch. Zero drivers.
Benefits of U2F Over Other 2FA

Protection against phishing and MitM

One device, many sites, with no shared secrets

Open standard, platform/browser support (no client, no driver)
U2F - Universal 2nd Factor
Stats from Google deployment

U2F vs Google Authenticator

● 4x faster to login
● Support reduced by 40%
● Significant fraud reduction
# U2F ecosystem

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Online services</td>
<td>Google, GitHub, Dropbox, PushCoin</td>
</tr>
<tr>
<td>Chip providers</td>
<td>ARM, Infineon, NXP, GT2</td>
</tr>
<tr>
<td>Device providers</td>
<td>FEITIAN, egis, yubico, HAPPLINK</td>
</tr>
<tr>
<td>Biometrics technology</td>
<td>eyeLock, Sonavation</td>
</tr>
<tr>
<td>Enterprise servers</td>
<td>Duo, Entersekt, Nok, RCDevs</td>
</tr>
<tr>
<td>Open source sw/servers</td>
<td>Google, yubico, WordPress, Shibboleth</td>
</tr>
<tr>
<td>Mobile apps &amp; clients</td>
<td>Entersekt, Google, Android</td>
</tr>
<tr>
<td>Browsers</td>
<td>Chrome, Firefox</td>
</tr>
</tbody>
</table>
Sample U2F authenticators

Form factors: Keychain devices, cards, wearables

Transports: USB, NFC, Bluetooth

Token-less options: Security chips in computers/phones, mobile client only

1st factor options: PIN/passwords, biometrics, geo location, etc.
<table>
<thead>
<tr>
<th>Registration</th>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Server sends challenge</td>
<td>1. Server sends challenge + key handle</td>
</tr>
<tr>
<td>2. Device generates key pair</td>
<td>2. Device unwraps/derives private key from key handle</td>
</tr>
<tr>
<td>3. Device creates key handle</td>
<td>3. Device signs challenge + client info</td>
</tr>
<tr>
<td>4. Device signs challenge + client info</td>
<td>4. Server receives and verifies using stored public key</td>
</tr>
<tr>
<td>5. Server receives and verifies device signature using attestation cert</td>
<td></td>
</tr>
<tr>
<td>6. Key handle and public key are stored in database</td>
<td></td>
</tr>
</tbody>
</table>
U2F Entities

User Side

U2F Authenticator

User Action

Secure U2F Element (optional)

Transport

USB (HID)
NFC
Bluetooth

FIDO Client Browser

U2F JS API

U2F Code

USB (HID) API
NFC API
Bluetooth API

Relying Party

Web Application

U2F Library

Public Keys + Key Handles + Certificates
Adding U2F Support

Original Database

<table>
<thead>
<tr>
<th>user_id</th>
<th>Password#</th>
</tr>
</thead>
<tbody>
<tr>
<td>JohnDoe</td>
<td>4^hfd;`gpo</td>
</tr>
</tbody>
</table>

U2F Database

<table>
<thead>
<tr>
<th>user_id</th>
<th>Meta</th>
<th>U2F Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>JohnDoe</td>
<td>Yubico, Security Key, USB</td>
<td>Key handle, public key, certificate</td>
</tr>
<tr>
<td>JohnDoe</td>
<td>Yubico, YubiKey NEO, USB + NFC</td>
<td>Key handle, public key, certificate</td>
</tr>
</tbody>
</table>
# YubiKey Offerings

## Services
- Support
- Validation Services
- Customization Services

## Products
- **U2F Security Key** (Single Protocol) $18
- **YubiKey NEO** (All Protocols) $50
- **YubiHSM** (For Servers) $500

## Software
- Public Key
  - U2F, PIV, OpenPGP
- Driverless OTP
  - OATH, YubiKey
- HSM
  - Securing Servers

## Hardware
- **USB**: Nano Form
- **USB & NFC**: Keychain Form
Try U2F

Contact edu@yubico.com if you would like to...

- Get a free YubiKey NEO for your test and evaluation purposes.
- Receive upcoming U2F developments incl. mobile apps, Mozilla support, Shibboleth plugin, etc.

For a discounted U2F Security key for use with Google for Edu/Work please go to https://www.yubico.com/gafw/
# Feature Comparison

<table>
<thead>
<tr>
<th>Features</th>
<th>U2F</th>
<th>Smartcard</th>
<th>OTP token</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protects against phishing &amp; man-in-the-middle</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instant “one touch” user experience</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>No readers, drivers, client software</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>One device to many independent services</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>No time synchronization issues</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crush resistant, no batteries</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User presence sensor</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Self deployment</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>No cryptographic secrets stored/hosted/shared</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
U2F Resources

Minitwit tutorial code  
github.com/dainnilsson/flask-u2f-tutorial

Yubico U2F demo server  
demo.yubico.com/u2f

Libraries, plugins, sample code  
dev.yubi.co/U2F

Yubico U2FVAL service  
u2fval.appspot.com

Standalone U2FVAL server (and docs)  
dev.yubi.co/u2fval
IAM Online Evaluation

Please complete a short evaluation of today’s presentation

InCommon Shibboleth Installation Workshops

February 4-5. 2016 – MCNC – Durham, North Carolina
   Registration is open at www.incommon.org/shibtraining

April 14-15, 2016 (tentative) – TBA

May 19-20, 2016 – University of Chicago
   Registration not yet open

www.incommon.org/shibtraining
Upcoming Webinars

Monday, Nov. 16, 2015 – 2 pm ET - Introduction to Interfederation

Wednesday, Nov. 18, 2015 – 2 pm ET - Technical Implementation of Interfederation

Friday, Dec. 11, 2015 – 1 pm ET - Policy and Legal Considerations for Interfederation

www.incommon.org/edugain

Next IAM Online

Tuesday, Dec. 8, 2015 – 4 pm ET - The Future of Federation: Interfed, K-12, Demographic Shifts and InCommon

www.incommon.org/iamonline