Password-less Strong Authentication

OWASP, Dallas, TX, May 17th 2016
Be Secure with No Passwords

Girish Chiruvolu, Ph.D., MBA, CISSP, CISM
Information Security and Risk Management
How Would You Choose Your Team?

Every member is a STRONG one to ride rough waters
Familiar?

Anthem healthcare system was breached by attackers’ software February 19, 2014

1.5 million accounts compromised June 2014

Sony pictures hacked – loss of revenue and disclosure of internal employee information May 2014

More than 2 million credit cards compromised Sept 2014

The entire Ashley-Madison business operations paralyzed June 2015

1.5 million accounts compromised June 2014

Hackers in got credit and debit card numbers and sensitive information April 2014
Evolution of Cyber Security Threatscape

**1988**
- **FUN**
  - Technically curious individuals

**2001**
- **FAME**
  - Technically adept groups leaving their mark on public websites

**2004**
- **FORTUNE**
  - Cyber criminals and organized gangs stealing money, data ransom schemes and competitive information

**2010**
- **FORCE**
  - Nation states and non-nation state groups launching targeted attacks for strategic purposes

**Nature of Threat**

- Academic
- “Script Kiddies”
- Commodity Threats
- Advanced Persistent Threats (APT) – Targeting Government Entities
- APT – Targeting Private Sector
Authentication Jungle

What is your pet's name?

Late 1980s 1990s 2000s and beyond
Online Identity and Why So Important?

"On the Internet, nobody knows you're a dog."

$5.9 B online fraud in '14
How do You Establish Online Identity?

User-ID
- Your user-id identifies who you are "potentially"
  - is established by a set of information identity attributes by which an individual is definitively distinguished within a context.

Password
- Your password confirms "potentially" you are the right person

Still unsure?
- Further risk assessment?
- Use additional mechanisms to have "more" confidence in the "trust" being established with the online ID
Information Security and Risk Management

Security Policy
Directory
Governance
Logon
Provisioning
Authentication
Authorization
Access Control
Analysis
Development
Mobility
Data Quality
Audit
Reporting
Good Authentication is all about Balancing

Zero client footprint & easy to use

Low cost of implementation & maintenance

Robust security with device-less disposable password; resilient to Man-in-Middle attacks, etc.

Cost

Security

Convenience
Good Characteristics of Online Authentication

- Secrecy and hard to spoof
- Repeatability
- Mutual trust
- Convenience

Cost-effective

Scalable

Resiliency to attacks
- Off-line dictionary attacks
- Online attacks-
  - Phishing,
  - Over-the-shoulder,
  - Key-logging,
  MiM/Sniffing
Closer Look at Passwords!

- Strong Passwords hard to remember – I%&killer$#144Pwd+
- “Social engineering”
- Finding written password: Post-It Notes
- Guessing password: Spouse/Kid DoBs etc.
- Shoulder surfing
- Keystroke logging
  - Virtual keyboards/mouse
- Screen scraping (with Keystroke logging)
- Brute force password crackers (Rainbow tables – hash tables, salts)
- **Password explosion** (SSO and Fed-SSO)

English has a maximum entropy of 6 bits per character

Typical pure random password of 6 characters = 36 bits of entropy

Typical human generated passwords → Much less entropy

My password: letMe1in
The SOS Signal on (1st Factor) Passwords

At least $1B Online Fraud Annually

Average = $120/online user*

*Sources: RSA annual report 2014
Industry Quotes

• “Passwords are like toothbrushes....
You don’t lend them out
and you change them often!”

Wayne Kissinger, Banking Professional
## Multi-Factor Knight!

<table>
<thead>
<tr>
<th>Method</th>
<th>Examples</th>
<th>Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>What you know</td>
<td>User Ids, PINs, Passwords</td>
<td>Shared</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Easy to guess</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Usually forgotten</td>
</tr>
<tr>
<td>What you have</td>
<td>Cards, Badges, Keys</td>
<td>Shared</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can be duplicated</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lost or Stolen</td>
</tr>
<tr>
<td>Something unique about user</td>
<td>Fingerprint, face, voiceprint, iris scan</td>
<td>Not possible to share</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Repudiation unlikely</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Forging difficult</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cannot be lost or stolen</td>
</tr>
</tbody>
</table>
Why Choose A Weak Factor (team member)?

Strengthen your MFA with ALL Strong Factors
The Multifactor Authentication Frenzy

• To support a weak foundation, need several props

• MFA achieves the same goal

Password

Second Factors
Email, SMS, OTP, Tokens

Third Factors
Fingerprint, Iris, Voice, Face

Fourth and Fifth Factors
Space, Time, Abstract??
Biometrics

Face, Finger, Iris, Palm, Retina, Signature, Voice

FAR: False Acceptance Rate
FRR: False Rejection Rate
EER (also Cross-over): Equal Error Rate
## Comparison

<table>
<thead>
<tr>
<th>Biometric Type</th>
<th>Accuracy</th>
<th>Ease of Use</th>
<th>User Acceptance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>High</td>
<td>Medium</td>
<td>High (if device local) ; Low</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Voice</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Retina</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Iris</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Signature</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Face</td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
Fast Identity Online (FIDO): UAF and U2F

Universal Access Factor
- Local device authentication (agent)
- Cloud application needs to trust the result of UAF agent on local device

U2F
- Still needs a password
- Either USB Key chain or Bluetooth (others evolving)
How does FIDO UAF* work?

FIDO Authenticators

PKI-based
Private Keychain at user end;
user-public key on the server

FIDO SERVER

*Universal Authentication Framework
FIDO – Potential issues

- U2F is not zero footprint
- Transaction challenge is still cumbersome
- Even though there is provision on formulating policies over which devices and UAF/U2F, FIDO server accepts
  - Untrusted User Agent
  - Responsibility lies with server to determine unknown risks at user end
- If server is compromised, could replace the public keys for the users (denial of service)
  - No additional public key validation to trust beyond bootstrapped registration
- Device lost – is painful; all keys are tied in
  - Similar to forgot password flow (traditionally the weakest link)
Can we Do better Than Passwords for 1\textsuperscript{st} Factor?

Focus: Stronger 1\textsuperscript{st} Factor beyond passwords

Wide Wild World of Cyber Space

2\textsuperscript{nd} Factor: What you have: Token/SMS Phone

3\textsuperscript{rd} Factor: What you are: Biometrics
Closer Look At First Factor Authentication

• First Factor only implies “What you know”
  » Not necessarily ≠ “PASSWORD”

• User response Can be dynamic (changing)

• No additional gadgets needed! – All in the brain

• Cannot be revealed until User chooses to
  » Willingly or Otherwise

– Independently and uniquely can be chosen by the User
– Typically depends on other technologies for Mutual Authentication
  • Need not be!
Why First-Factor (knowledge) is indispensable?

- Knowledge-base cost $0 capex
- Zero-footprint - Nothing to carry around or maintain – all in the brain
- Convenient
- Still do not have confidence in “what you have” and “what you are” – Absolutely not fool-proof

- Note: First factor always ≠ Password
- First factor merely says “What you know”
  - How you do
  - What you do
    - Optional
Simple Hybrid-Zero-Knowledge Processing (SHZKPP)

A zero-knowledge password proof (ZKPP) is an interactive method for one party (the prover) to prove to another party (the verifier) that it knows a value of a password, without revealing password to the verifier.

ZKPP is defined in IEEE 1363.2 as "An interactive zero knowledge proof of knowledge of password-derived data shared between a prover and the corresponding verifier."

Why Simple & Hybrid (explicit and implicit secrets) ZKPP?

• Zero-footprint — Practically what humans can do
• Retain password user-experience
How does it work?

Answer: 43

OTP: jjetw427$2&dse+@
+ Shared secret1 (txt)

Answer: 48

OTP: dj,ey12c4r844#f
+ Shared secret2 (txt)
Reverse-Turing Test-based & Probability

\[ P(A_1 A_2 A_3 \ldots A_n) = \prod_{i=1..n} P(A_i) \]

Probability of manual cracking approaches \( \sim 0 \) (zero)
Key Highlights of the SHZKPP schemes

- **OTP**
  - In-Band
  - Don’t need another cellphone or channel

- **Several orders security over key-loggers**
  - Passwords offer zero protection against key-loggers

- **Server-controlled authentication process**
  - Passcodes don’t exist until generated

- **Zero-footprint & Mutual authentication**
  - Nothing seriously to lug around

- **Secrets never travel over the Internet**
  - Only processed result of challenge data

- **Scalable and repeatable framework**
  - Strength and complexity proportional to noise
Containing Credential Explosion: Single-Sign On (SSO)

- As number of protected applications increase, passwords also increase.
- Average need of around 20 passwords in day-to-day life.
- Humans can at best remember 6 secrets.

Within Enterprise SSO and across Enterprises (Federated SSO)
## Major Mechanisms of SSO

<table>
<thead>
<tr>
<th></th>
<th>OpenID</th>
<th>OAuth</th>
<th>SAML</th>
<th>OpenID Connect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dates from</td>
<td>2007</td>
<td>2006</td>
<td>2002</td>
<td>2010</td>
</tr>
<tr>
<td>Current version</td>
<td>OpenID 2.0</td>
<td>OAuth 2.0</td>
<td>SAML 2.0</td>
<td>OpenID Connect 1.0 (new)</td>
</tr>
<tr>
<td>Main purpose</td>
<td>Single sign-on for consumers</td>
<td>API authorization between applications</td>
<td>Single sign-on for enterprise users</td>
<td>Combine OpenID authentication identification and Oauth authorization</td>
</tr>
<tr>
<td>Protocols used</td>
<td>XRDS, HTTP</td>
<td>JSON, HTTP</td>
<td>SAM, XML, HTTP, SOAP</td>
<td>JSON, HTTP</td>
</tr>
</tbody>
</table>
Summary

• Passwords the frontline authentication mechanism is fragile
  – Many hacks and attacks – almost a broken technology
• Second and Third factor authentication mechanisms depend either on carrying a gadget or susceptible to errors – technology advances improving

• Zero-footprint dynamic disposable passcodes can balance the complexity and scalability while retaining password experience
  – SSO further reduces the need to multiple credentials
• As ever, layered approach with compensating controls suggested
Q & A? Thank you!
U2F is an open 2-factor authentication standard that enables:
- keychain devices, mobile phones and other devices
- securely access any number of web-based services

The U2F specifications are today hosted by the FIDO Alliance (http://fidoalliance.org/specifications/download)
Quick Lingo

**SAML**

- **Assertion**
  - Data by vouching authority on authentication or any attribute of the user including authorization scope of a resource

- **Binding**
  - Mapping of elements from protocol1 to protocol2

- **Profiles**
  - A set of rules usage of assertions or protocol messages usage or mapping of attributes

**Oauth**

- **Tokens**
  - Access tokens are credentials used to access protected resources; similarly refresh tokens are credential used to get access token to access a resource

- **Authorization grant**
  - After verification of user credentials and consent of resource utilization issued authorization grant

- **Resource**
  - A protected resource for which access it requested.
SAML 2.0 – Web SSO Protocol

- Service provider generates a SAML request and redirects to IDP
- IDP authenticates and asserts user profile and issues SAML token
- Service provider grants access to resource after verification
OAuth example
Oauth 2 Flow

- Resource request translates into authentication and authorization and access token
- Resource consumer can use the resource until token expires
- Can be refreshed or reissued depending on policy