NCCoE: Mobile App Single-Sign On

Achieving a secure, reliable, accessible SSO solution for Public Safety & First Responders
Introductions

- Bill Fisher – NIST, National Cybersecurity Center of Excellence
- Mike Korus – Motorola Solutions
- John Bradley – Ping Identity
- Arshad Noor – StrongAuth
- Mark Russell – MITRE Corporation
Challenge
Project Challenge

• Mobile platforms offer a significant operational advantage to public safety stakeholders by providing access to mission critical information.

• These advantages can be limited if complex authentication requirements hinder PSFR personnel, especially when delay – even seconds – is a matter of containing or exacerbating an emergency situation.
Security Challenge - Passwords

Passwords:
• Complexity - hard to remember
• Hard to type on mobile phone
• Need one for each application
• They are often re-used
• Can be phished

Source: https://xkcd.com/936/
Solution
Core of the Build

Multifactor Authentication to Mobile Resources

• Biometrics, external hardware authenticators and other authentication options

Single Sign-on to Mobile Resources

• Authenticate once with mobile native app or web apps
• Leverage initial MFA when accessing multiple applications

p@$$w0rd +
Benefits of an NCCoE Reference Design
NCCoE Benefits – Industry Collaboration

NCCoE brings in Industry experts to design and build the reference design:

Mobile SSO Technology Vendor Build Team:
NCCoE Benefits – Standards Based

NCCoE solutions implement standards and best practices:

Using modern commercially available technology:
NCCoE Benefits – Practical Guidance

• Project will result in a freely available NIST Cybersecurity Practice Guide (SP 1800-x) including:

- Technical Decisions
- Trade-offs
- Lessons Learned
- Build Instructions
- Functional Tests
Value to PSFR Community
Value to PSFR Personnel

**Efficiency**
Save time and efficiency by reducing the need to authenticate to multiple mobile applications individually

**Simplicity**
Allowing a user to manage less username/password credentials

**Flexibility**
Multiple options for multifactor authentication
Value to PSFR Organizations

**Modern**
Solution takes advantage of the latest commercially available mobile technology and best practices

**Interoperable**
Technology uses standard protocols and flows to improve interoperability

**Security**
Architecture designed with security characteristics as core requirement (more on this later)

**Cost Savings**
Reduction in costs - NCCoE delivers requirements, architecture and a reference implementation
Solving Mobile App Single Sign-On Using Standards
IETF BCP – “OAuth 2.0 for Native Apps”

- Implements standards such as OAuth (RFC6749) and Proof Code for Key Exchange (PCKE - RFC7636)
- User's password and other credentials are never exposed to the SaaS provider or mobile app
- Apps get an OAuth Token with limited scope of authorization - apps only get access to back-end systems they should be accessing
- IdP policy controls which user attributes are shared with the SaaS provider
- PKCE prevents malicious apps on the device from intercepting the authorization code and using it to get access tokens
- Agnostic to the Authenticator (OIDC, SAML, etc...)
AppAuth Software Development Kit

Benefits of AppAuth

- Implementation of the “OAuth 2.0 for Native Apps” BCP
- Developed by OpenID Foundation
- Free and open source
  - Code maintained by Google for both iOS and Android
- Securely implements standards
- Developers can “Drag and Drop” into a mobile app
Standards-Based Multifactor Authentication
Introduction to Fast Identity Online (FIDO)

Passwordless Experience

Second Factor Experience

Flexible authentication spanning any number of service providers

*slide taken from FIDO Presentation to NCCoE 5/31/2017
MFA using External Authenticator via FIDO U2F

FIDO U2F – External Authentication over NFC

- U2F token used in addition to primary authenticator (e.g., password)
- "FIDO protocols mandate a “proof of user presence” (e.g., by pushing a button, verifying your biometric data, etc.)”
- IdP may support the protocol directly (natively or using a plug-in)
- Authenticator attestation sent at time of registration & authentication – IdP can decide whether or not the authenticator is acceptable
MFA using FIDO Universal Authentication Framework

FIDO UAF is Multifactor Authentication

• Factor 1: User verification (one or more user tests)
• Factor 2: Public Key cryptography challenge/response

FIDO UAF Registration defines how Keys are generated and enrolled

• IdP can send policies during registration identifying authenticator criteria (manufacturer, security characteristics, modalities, etc.)
• Then Device generates keys BUT only registers the PUBLIC key (Private key kept private)
• Username, user verification, key, IdP (relying party) are bound together.
Benefits of FIDO

- Standards Based
- No Secrets on the Server Side
- Biometric Data (if used) Never Leaves Device
- No Phishing

*slide taken from FIDO Presentation to NCCoE 5/31/2017*
Simple Example
High Level Components

Technologies

Software as a Service (SaaS)
- This approach uses centrally-hosted software that is provided “on demand”, includes apps and back-end servers

OpenID Provider
- Server used to manage user identities and roles, and to share user info with other organizations

Authorization Server
- Server used by SaaS provider to communicate with an OpenID Provider and authorize users

Fast Identity Online (FIDO)
- Work-in-progress: This protocol, and hardware that uses it, allows users to sign on w/ tokens instead of passwords

Actors

Central Public Safety Service Provider (CPSSP)
- Represents a SaaS provider that hosts a back-end for mobile apps used by the PSFR community
- This may or may not be the same entity that writes the mobile client apps

Local Public Safety Department (LPSD)
- Represents a local Police, Fire, EMS, or other public safety or first responder organization that uses the services provided by CPSSP
- This organization manages user accounts and has an OpenID Provider for authentication
Simple SSO Scenario

1. User asks for Data
2. User Logs in
3. User Info
4. Return Data

FIRE DEPT

POLICE DEPT

OTHER SaaS PROVIDERS ACCEPT INITIAL LOG IN AND GRANT ACCESS.
Demonstration
Questions?
Project Resources

• Project Description Document:
  • Document has details architecture and flow diagrams

• Build Team Announcement & Blog:
  • Discusses products used in the build

• PSFR-NCCoE@nist.gov
  • Inquiries go directly to NIST project leads
Acronym List

API - Application Programming Interface
AS - Authorization Server (term specific to the OAUTH spec)
BCP - Best Current Practice
FIDO - Fast ID Online
FOSS - Free and Open Source
HTTPS - Hyper Text Transfer Protocol Secure
IDP - Identity Provider
IETF - Internet Engineering Task Force
LDAP - Lightweight Directory Access Protocol
NCCoE - National Cybersecurity Center of Excellence
NFC - Near Field Communication
OIDC - Open ID Connect
OAUTH - not an acronym, but a rights delegation protocol
PCKE - Proof Key for Code Exchange
PSFR - Public Safety First Responder
RFC - Request for Comment
RP = Relying Party
SaaS - Software as a Service
SAML - Security Assertion Mark-up Language
SDK - Software Development Kit
SP - Special Publication
SSO - Single Sign On
U2F - Universal Two Factor
UAF - Universal Authentication Framework