Expanding the SIM Card Use Prize Challenge: Overview and Demo

Mike Bartock - NIST Conor Patrick - SoloSim Matt Lourie – Nok Nok Labs Shane Weeden - IBM

#PSCR2020





DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately.

Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

* Please note, unless mentioned in reference to a NIST Publication, all information and data presented is preliminary/in-progress and subject to change

NIST

#PSCR2020



(...

Agenda

- Overview of the Prize Challenge
- Hear from the Prize Challenge Winner
- Hear from two Creative Research and Development Agreement partners
- See a demo of the winning solution

SoloSIM

Conor Patrick

Founder, **SoloKeys** @_conorpp

May 29, 2020

DISCLAIMER

This presentation was produced by guest speaker(s) and presented for publication in the National Institute of Standards and Technology's PSCR 2020: The Digital Experience. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government

Posted with Permission.



#PSCR2020



6.44

Finding out about SIM Card Challenge



SoloKeys makes open source FIDO2 products, looking to expand open source platform (e.g. SIM card/smart cards).

Learned about SIM Card Challenge at HardwareCon.

Had a lot of FIDO2 authenticator knowledge, and learning about SIMs + solving authentication problems for a new market could be a great opportunity.

Designing the solution



ARAM is provisioned on UICC for Android OS to give SoloSIM access to UICC.

Overall design from the beginning.

App implements FIDO2 authenticator (CTAP) with SIM/UICC as a secure element.

App implements FIDO2 client + APIs to demo on multiple FIDO2 servers.

SIM Card

Biggest high level challenge is with the SIM card.

- Current SIM will not have "HSM" features to implement FIDO2.
- Political issue; not allowed to put custom apps on SIM.

Next best option for demonstration: **SIM overlay**.



Development challenges

Android restricts access to SIM card.

- SIM card needs to have a standard set of "access rules" installed
 - Tells Android what signed apps are allowed to interact.
- Debugging required building and installing custom Android ROMs.

(**iOS** likely has similar API + restrictions, but it is undocumented).

FIDO2 interoperability. Many cryptographic elements and types of encodings at play. Difficult to see & figure out what is wrong.

- Thankfully the transport binding API was used for both IBM & NokNok

Overall experience

- Great challenge
 - Developing flexible/mobile/interoperating root of trust is a much needed solution
 - Opportunity provided by NIST PSCR went very well overall

- Work is ongoing
 - Still restrictions with using with SIM cards.
 - Makes bottom-up/startup approaches difficult.
 - Short term:
 - SoloSIM (now "Authim") now focusing on evidence authenticity app solution.
 - Long term:
 - SoloKeys focusing more making an open platform for smart cards.
 - Making an open & Global Platform compliant device that can run applets.
 - Open USIM + eSIM apps.

Use of funds

\$37.5k awarded, \$4k of which is for business development.

~ \$3k

- Coworking space
- Travel costs; Going to CES
- Incorporation fees
- More phones for testing + development

~ \$5k

- Reinvesting in new IP (evidence authenticity app for first responders).
 - Funding development
 - Teamed up with another developer
 - Make automatic way to take evidence + using root of trust on phone.

Thank you!

If you have any questions, please email me directly at conor@solokeys.com

nok

The Trusted Leader in Passwordless Authentication

PSCR

Matt Lourie Sr. Director of Engineering

DISCLAIMER

This presentation was produced by guest speaker(s) and presented for publication in the National Institute of Standards and Technology's PSCR 2020: The Digital Experience. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government

Posted with Permission.



#PSCR2020



6.44



- About Nok Nok
- S3 Authentication Platform
- How Contestants used Authentication Service





Who is Nok Nok?



- Deep domain expertise in FIDO next-generation authentication
 - We invented FIDO (ex-PGP team)
 - Experts in Consumer Authentication



- Most widely deployed B-to-C passwordless solution
 - 200M+ Users
 - Billions of authentications



- Proven technology with innovations based on the real world
 - Servers deployed globally at scale
 - More than 90 US- and International patents issued or filed



Simple, Strong, Scalable Any App, Any Device, Any Authenticator

NIST / Nok Nok Partnership

- Bill Fisher (NIST) introduced Nok Nok to NIST in 2014
- Nok Nok collaborated with National Cybersecurity Center of Excellence (NCCoE) on Mobile Single Sign On using FIDO
- Nok Nok solution for First Responders highlighted in NIST Webinar in 2017
- Nok Nok has deep knowledge of authentication needs of Public Safety communication solutions



Why FIDO?

Industry Standard

- Interoperable, secure approach
- Certification program for compliance
- Global standard supporting regulatory requirements, e.g. PSD2 SCA, eIDAS

Secure

- No shared secrets
- Leverages public key cryptography

Privacy Preserving

Only public keys stored on server

Cost Effective

Reduced operational complexity and costs

Combine optimal security with optimal convenience



Nok Nok Delivers Many Business Advantages

Improve Customer Experience

Reduce Costs



- Improve onboarding success rate
- Improve authentication speed
- Reduce transaction
 abandonment



- Reduce call center costs due to password resets
- Reduce SMS OTP costs
- Reduce development costs
 to support MFA

Meet Regulatory Requirements and Reduce Fraud



- Meet PSD2 SCA requirements
- Reduce ATO
- Reduce phishing attacks
- Reduce man-in-the-middle
 attacks



Global Brands Trust Nok Nok for Their Solution





∩ok







Global Partners Rely on Nok Nok for Authentication



S3 Authentication Suite Architecture





Contestant Setup using Cloud Service

- Product supports both on-premise and cloud deployment
- For simplicity, contestants were set up in the cloud
- Contestants used REST API Integration
- Federation Connectors are also supported



Administration – Authenticator Policies

nok si nok si	ERVER ADMINISTRA	ATION Analyti	cs	Management		Help	Tenant: default
Properties	Authenticator Policies	Recovery Policies	Au	uthenticator Metadata	User Management	Locations	Encryption Keys

Search:

Policies

♠ Import...
♠ Export Active...
● Add Policy

Show 10 ✓ entries

Policy A	Modified \$	Status 🌲	Actions
default This is a sample default advanced policy definition	Dec 6, 2017 7:20:20 PM	ACTIVE	🕜 42 क़ 前
policy1 This is a sample default advanced policy definition with webAuthn	Aug 7, 2019 10:05:24 PM	ACTIVE	2 4 Ф 前
policy2 This is a sample default advanced policy definition with webAuthn	Aug 7, 2019 10:05:26 PM	ACTIVE	2 4 Ф 前
policy3 This is a sample default advanced policy definition with webAuthn	Aug 7, 2019 10:05:28 PM	ACTIVE	2 4 Ф 前
policy4 This is a sample default advanced policy definition with webAuthn	Aug 7, 2019 10:05:31 PM	ACTIVE	2 4 🕈 💼



Administration – Analytics





Contestant Administration: Drill Down

Authentication

ID	Device Name	Device Model [?]	os	Manufacturer	Authenticator	Authenticator Description	Timestamp	Country	Status Code
abcdef12345g hijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a- 11e9-9cb5- 2a2ae2dbcce4	solokeys_user	12/3/2019, 8:16:17 AM	Unknown	ок
abcdef12345g hijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a- 11e9-9cb5- 2a2ae2dbcce4	solokeys_user	12/10/2019, 7:33:46 AM	Unknown	ок
abcdef12345g hijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a- 11e9-9cb5- 2a2ae2dbcce4	solokeys_user	1/8/2020, 11:37:59 AM	Unknown	ок
abcdef12345g hijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a- 11e9-9cb5- 2a2ae2dbcce4	solokeys_user	1/8/2020, 10:11:36 AM	Unknown	ок
abcdef12345g hijkl	NNL's device	NNL's model	NNL's OS	-	2ef16fde-bf5a- 11e9-9cb5- 2a2ae2dbcce4	solokeys_user	12/2/2019, 12:16:41 PM	Unknown	ок
More									



FIDO Registration with SIM Card





FIDO Authentication with SIM Card









IBM Security - industry outreach with NIST



IBM Security

Expanding the SIM Card Use for Public Safety



Shane Weeden Senior Technical Staff Member





DISCLAIMER

This presentation was produced by guest speaker(s) and presented for publication in the National Institute of Standards and Technology's PSCR 2020: The Digital Experience. The contents of this presentation do not necessarily reflect the views or policies of the National Institute of Standards and Technology or the U.S. Government

Posted with Permission.



#PSCR2020



6.44



IBM Security / © 2020 IBM Corporation

Hundreds of open integrations at the center of your ecosystem



The industry's broadest and most complete security portfolio



Advance Security Maturity

- Strategy and Planning
- Risk Assessments
- Advisory Services

Build Leadership and Culture

- IBM Security Command Center
- IBM Security Command Mobile
- IBM Security Command Onsite
- IBM Security Command Virtual



Stop Advanced Threats

- Security Operations Consulting
- X-Force Threat Management
 Services
- X-Force Red
- QRadar

Orchestrate Incident Response

- Resilient
- X-Force IRIS

Master Threat Hunting

- i2 Intelligence Analysis
- QRadar Advisor with Watson



Protect Critical Assets

- SDLC Consulting
- Data Protection Services
- Guardium
- Data Risk Manager
- Multi-cloud Encryption
- Key Lifecycle Manager

Deliver Digital Identity Trust

- Trusteer
- Verify

Govern Users and Identities

- Identity Management Services
- Identity Governance
- Verify
- Verify Access
- Secret Server

Unify Endpoint Management

- Endpoint Management Services
- MaaS360

Secure the journey to cloud

Cloud Pak for Security | Cloud Security Services | Cloud Security Products

Smart Identity for the Hybrid Multicloud World

Securely connecting every user, API, and device to every app in and outside the enterprise



IBM Security Verify: Smart Identity for the Hybrid Multicloud World

Serving both workforce and consumer populations



Single Sign On (SSO): One-click access Eliminate password hassles with a unified application launch pad and SSO from any device, to any cloud or on-premises application



Multi Factor Authentication (MFA): 2FA to any target system Protect web, cloud, mobile, VPNs, and operating systems with a common platform for MFA, including passwordless technologies such as FIDO2



Governance: User lifecycle management and compliance Request, approve, provision, and periodically recertify user access to applications



Adaptive Access: Balance security and convenience Dynamically assess full user, device, and environment context for an AI-powered, aggregated risk score, and enforce MFA when risk is high



Analytics: Mitigate identity-related risks through a holistic view of IAM data Process activity and entitlement data from a variety of sources, providing a 360 view of access risks with the ability to take action based on those risk insights

Supporting NIST participants with IBM Security Verify Access

C 🔒 nistfido2.securitypoc.com/mgaauth/sps/mga/user/mgmt/html/device/fido2_registrations.html

TEM.

FIDO2 Registrations

Welcome: Shane Weeden Logout Home

Existing Registrations

Register Authenticator

	Friendly Name	Vendor Description	Vendor Icon	Operation
	Shane Weeden 20042020083755	IBM NIST FIDO2 Public Safety Challenge		Details Test Remove
	Shane's Pi Camera	IBM NIST FIDO2 Public Safety Challenge		Details Test Remove
	lew Registration	ons (e.g. to select resident key)		

		Postma	n				
🕂 New Import Runner 📑 🔻		👪 My Workspac	e 🔻 🔒 Invite		8 K F	🜲 🎔 Sign In	
Q Filter	POST WhoAml	× Pos	FetchAttesationOption	15 + •••	NISTFIDO2-Participant	• © ‡	
History Collections APIs	▶ WhoAmI				Comments 0	Examples 0 🔻	
+ New Collection Trash	POST	<pre>r https://{{hostport}}/m</pre>	gaauth/sps/apiauthsv	c/policy/whoami	Send	▼ Save ▼	
NISTFIDO2-Participant 7 requests	Params Aut	norization Headers	(13) Body ●	Pre-request Script	Tests Settings	Cookies Code	
POST WhoAml	Query Params						
POST FetchAttesationOptions	KEY		VALUE		DESCRIPTION	••• Bulk Edit	
POST PostAttesationResult	Key		Value		Description		
POST FetchAssertionOptions	Body Cookies (2) Headers (9) Test R	esults (🕼 Status: 200 OK T	ime: 1293 ms Size: 5.19 KB	Save Response 🔻	
POST PostAssertionResult	Pretty Rav	v Preview Visualiz	e JSON 🔻	-		Q	
POST FetchAssertionOptionUsernameless	1 4						
POST PostAssertionResultUsernameless	2 "a	uthenticated": true,					
Self Verify Tenant 50 requests	3 "u 4 "d 5 "c	3 "username": "sweeden@aul.ibm.com", 4 "displayName": "Shane Weeden", 5 "credJsonB64U": "usuBocmluXBLWMedi01+ZTmShbWM1005UVH11TividH1vZCT6TmN/ubionYm86bm5+ZYM6CVDC5U06NE4v0m5iX2)/zc "usuBocmluXBLWMedi01+ZTmShbWM1051UVH11TividH1vZCT6TmN/ubionYm86bm5+ZYM6CVDC5U06NE4v0m5iX2)/zc					
S Bootcamp 🖬 🖗 🕐							

• Simple easy-to-use web portal for viewing and managing FIDO2 registrations.

 Downloadable POSTMAN collection (and instructional video) containing a complete JavaScript implementation of a FIDO2 client.

Participants need only implement the algorithms available from the POSTMAN collection in their mobile phone application.



THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- 🗊 @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.



References:

- <u>https://www.nist.gov/ctl/pscr/open-innovation-prize-</u> <u>challenges/past-prize-challenges/2019-expanding-sim-card-</u> <u>use-public</u>
- <u>https://solokeys.com/</u>
- <u>https://noknok.com/</u>
- <u>https://www.ibm.com/blogs/sweeden/cloud-identity-fido2-</u> <u>consuming-fido2-as-a-service-from-ibm-cloud-identity/</u>

THANK YOU



#PSCR2020

