Duke Unlock
Passwordless Authentication with Shibboleth and WebAuthn

Shilen Patel
Architect, Identity Management

Mary McKee
Director, Identity Management & Security Services
Agenda

WHY
Passwords are a losing strategy.

WHAT
WebAuthn is and does.

HOW
We deployed Duke Unlock.

FUTURE
Scaling up and out.
WHY

Passwords are a losing strategy.
January 2018

We'll devise a password standard to keep Duke safe for years to come.

We'll do it with math!

" - us, in more innocent times
The Password Quagmire: What We Learned

- Humans (and thus, human-generated passwords) are predictable.

- Password cracking technology has evolved far beyond brute force, invalidating many traditional calculations of password strength.

- GPUs are really good at this kind of task.

- Compute power more accessible than ever.

- NIST shows most of our tactics are counterproductive.

https://pages.nist.gov/800-63-FAQ/
May 2018

So, about that safe and realistic password standard...

- us, profoundly humbled.
OPTION #1
Password managers for everyone
+ Already have tool
  - Have to convince all to use it
  - Political cost of forcing behavior change

OPTION #2
MFA for everyone, all the time
+ Proven results
  - Fatigue with current requirements
  - Telephony credit increase = $$$

OPTION #3
Device certificate authentication
+ Stanford's program is very impressive
  - Current infrastructure insufficient
  - Significant initial cost

OPTION #4
Paralysis by analysis
+ Lowest effort
  - Compromised sleep quality
  - Diminished pride in work and self

WINNER!
"What About WebAuthn?"
-Nick Tripp

WebAuthn at a Glance
• New standard for secure authentication
• Supports native authenticators
• Can combine factors for simple MFA
• Open-source, straightforward to explore

Nick Tripp at a Glance
• Manages Duke's IT Security Office
• Cracked "correcthorsebatterystaple" hash for $70 in cloud compute in ~24 hr
• Completely sober in this photo
WHAT
WebAuthn is and does.
FIDO2 Project

Objective: open authentication standard for strong, passwordless authentication.

Project comprised of:

- W3C Web Authentication API (WebAuthn)
- FIDO2 Client to Authentication Protocol (CTAP2)

https://fidoalliance.org/fido2/
WebAuthn Can Support

Native Authenticators (e.g., Touch ID)

Roaming Authenticators (e.g., YubiKey)

Single-factor Authn

Multi-factor Authn

Device Attestation (vendor, model, features)

Device Filtering/Selection (what will you accept?)
Wait, how is this multi-factor?

something you have
[registered device]

something you are
[fingerprint, facial recognition]

something you know
[PIN, gesture]

Uneasy with biometrics? Great! Don't use them. How you achieve MFA is between you and your device.
Authentication Flow

1. User visits website, is directed to Relying Party (RP), in our case, Shibboleth IdP
2. RP sends request: [ID, challenge, user verification requirements, list of registered credentials]
3. Browser validates origin, prompts for authenticator choice
4. User chooses authenticator and completes user verification
5. Authenticator creates assertion, signs data containing challenge, auth flags, etc.
6. Data returned to browser and sent to RP
Registration Process

1. **User provides** device nickname to web form, completes registration through familiar prompts by device

2. **Duke stores** user handle, credential type, credential id, public key COSE, signature count, attestation type, attestation data, registration time, nickname

3. **Shibboleth IdP prompts** for WebAuthn transaction on request
Early Testing

**FIRST: Guerrilla usability tests**

Dev team run, targeted IT staff, in-person registration only.

**NEXT: Actual usability tests**

Sent a professional into the field to conduct more formal testing.

**FINALLY: Remote, no-touch registration**

Sent invitation emails on request, hoped for the best.
Duke Unlock - Pilot Timeline

- **October 2018**: Initial proof of concept
- **March 2019**: WebAuthn specification finalized
- **July 2019**: Guerrilla registration/usability testing
- **September 2019**: Service branding session
- **October 2019**: Usability report in; self-service registration introduced
- **November 2019**: Duke Unlock version 2 released
HOW

We deployed Duke Unlock.
## Duke Unlock - Service Values

<table>
<thead>
<tr>
<th>SECURITY</th>
<th>COMMUNITY</th>
<th>THRIFT</th>
<th>PROGRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Expand coverage of MFA.</td>
<td>• Listen to feedback and</td>
<td>• Only invest in what people</td>
<td>• Skate to where the puck is</td>
</tr>
<tr>
<td></td>
<td>frustrations.</td>
<td>are responding to.</td>
<td>going.</td>
</tr>
<tr>
<td></td>
<td>• Increase user engagement on</td>
<td>• Scale MFA use without</td>
<td>• Embrace quickly changing tech</td>
</tr>
<tr>
<td></td>
<td>account security.</td>
<td>scaling MFA cost.</td>
<td>landscape.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Don't ask users to</td>
<td>• Engineer for tomorrow.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>increase $/time investment</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(BYO-MFA).</td>
<td></td>
</tr>
</tbody>
</table>

Duke Log In
You are on the correct Duke login page if the above begins

NetID
Current students, faculty, staff, sponsored guests

NetID
mkm16

Password

Forgot your password?

Go passwordless

Multi-factor Authentication

Duke Unlock v1

1. Type in NetID, tab out of field
   AJAX check for pilot participation

2. Click "Go Passwordless" link
   On registered and compatible devices/browsers

3. Complete login with browser

"Google Chrome" is trying to verify your identity on shib.oit.duke.edu.
Touch ID or enter your password to allow this.
Use Password... Cancel
Known Issues with v1
PROBLEM: USER GRASP

Branding Workshop

Lauren Hirsh, Information Architect at Duke

- Usability lead for project, overseeing testing, branding, and communications
- Led 2-hour session to develop service name and elevator pitch
- "Snuck up on me like a ninja" - anonymous Duke freshman
PROBLEM: USER ENGAGEMENT

Measuring Engagement

∑
All Users
Total registered users

Active Users
Recently used Duke Unlock

Registered, Not Active
Registered, but hasn't used recently

Word of Mouth Referrals
Registrations not related to campaigns
PROBLEM: USER ENGAGEMENT

Campaigns

Advertising for Duke Unlock has been limited to what will help us measure two things:

• Are people finding this relevant enough to tell their friends and colleagues to sign up?

• How could we improve?
PROBLEM: EASE OF REGISTRATION

Usability Research

USER FEEDBACK:

"I find it really useful. It really shortens the time it takes to log into sites."

"It just...works!"

"I have been using the passwordless login the past few weeks during the pilot and I love it. It is very convenient and fast."

"Honestly, this is like a quality of life upgrade."

"That's lit. I love it. Amazing."

"It's been really great"

TAKEAWAYS:

- Self-service most urgent
- On-board, and then re-on-board
- Need to set Duke Unlock as default behavior
Join the Duke Unlock Pilot

Multi-factor authentication doesn’t need to be multi-step. Duke Unlock opens the door to enhanced security and convenience, allowing you to log in to Duke services as easily as you unlock your phone or laptop.

After you register a personal device with Duke Unlock, you can skip using your password and second verification step when logging in to Duke sites from that device.

Eligibility
Duke Unlock uses a new technology standard that isn’t supported everywhere yet. You are a good candidate for the pilot if you use one of the following:

- Android with fingerprint enabled, running Chrome or Firefox
- Mac (High Sierra+) with Touch ID enabled, running Chrome (version 75+)
- Windows (version 1903+) with Windows Hello enabled, running Chrome, Firefox, Edge, or Brave

Join our community group for periodic updates on support for new devices/browsers and developments in growing Duke Unlock from a pilot to a mainstream offering.

Introducing Self-Service

1. Provide detail on supported devices and a step-by-step "how to use" page.

2. Introduce confirmation email for later reference/support details.

3. Show registered and last used timestamps to help with device management.
Fixing the Login Link

Problems identified in user testing:

- Sometimes people don't see link.
- Registration status check pushes link rendering too far down the login page; users start typing password out of muscle memory.
- Mobile users logging in infrequently forget about the option to use Duke Unlock.
- Inability to set default means unnecessary typing.

13. Position of/Not seeing “Go Passwordless” link. (f=5) (SEVERITY: 3)
Description: User does not see the “Go Passwordless” link (frequently looking in the MFA options) or accidentally clicked the “Forgot your password?” link because of its proximity to the Go Passwordless link.

Recommendation(s) for consideration: Enable Duke Unlock as default or put the link before the Password input box (makes sense for context/tab order). (Could try either putting the link either right below the net id or shortening NetID input box and putting next to it.)

17. Typing password. (f=5) (SEVERITY: 2)
Description: User types in password before realizing/remembering to click the “Go Passwordless” link (Related to issue “Position of/Not seeing Go Passwordless link”).

Recommendation(s) for consideration: Enable Duke Unlock as default or put the link before the Password input box (makes sense for context/tab order). (Could try either putting the link either right below the net id or shortening NetID input box and putting next to it.)

25. Forgetting to use the service. (f=5) (SEVERITY: 0)
Description: User mentions they do not use the service every time they log in on a registered device because they frequently forget they have the option.
PROBLEM: REMEMBERING TO USE

Fixing the Login Link

Make link part of on-boarding
You are on the correct Duke login page if the above begins with: https://shib.oit.duke.edu.

**NetID**
Current students, faculty, staff, sponsored guests

Continue with Duke Unlock

Log in as mkm16

use password instead

For assistance, please visit oit.duke.edu/help or dhts.duke.edu.

**Duke Unlock v2**

1. Click.
   Button remembering Unlock preference

2. Tap.
   Native or roaming authenticator

3. Done.

No context switch.
MFA in less than one second.
FUTURE

Scaling up and out.
Metrics and Research Areas

Recruitment Materials
- How interested are people when they hear it?
- How well can people articulate what Duke Unlock does after a 5 second pitch?

Registration
- How effectively do users identify compatible devices?
- What is the success rate for registration?
- How often do people need to re-register the same device?
- How often does someone register and never use?

User Experience
- Do registered users ever choose not to use Duke Unlock?
- Do people share the service with others?
Removing Barriers at Duke

**Awareness Efforts**
- Circulate Duke Stores support among departments.
- Incorporate into password parties.
- Advertise on MFA site.

**Regular Deployments**
- Timely upgrades for best device support.
- Consistent UI refinements.

**Work with IT Support**
- Make sure support staff can use and provide feedback.
- Lobby for enablement of Windows Hello on managed devices.

**Circulate Tokens**
- Distribute biometric and NFC tokens to testers w/o native authenticators.
Track community developments

iOS Support
This is currently the biggest gap and most requested item from our community. Progress is encouraging, but only single-factor support is available today.

Bluetooth Support
Ability to use a phone as an authenticator would provide flexibility.

Security keys with biometrics
PINs on security keys are not convenient. Testing with biometric security keys has been promising.

OpenSSH and FIDO
Experimental support shows promise for wider application of the technology
Some Lessons Learned so far

Sigh....

- We were VERY naïve about how many people save passwords in their browser.
- Many people who have compatible devices have never activated Touch ID or Windows Hello, need to be walked through this.
- People really struggle with giving a personal device a nickname that will make sense to them later.

Yay!!!

- People who aren't very engaged on account security are often particular about device security. We can better align our interests.
- Students LOVE Duke Unlock, and are our fastest growing user population despite not specifically marketing to them.
- Mary's Yubikey broke 2 months ago and she hasn't felt the need to replace it.
Thank You!

Questions?