



# 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.

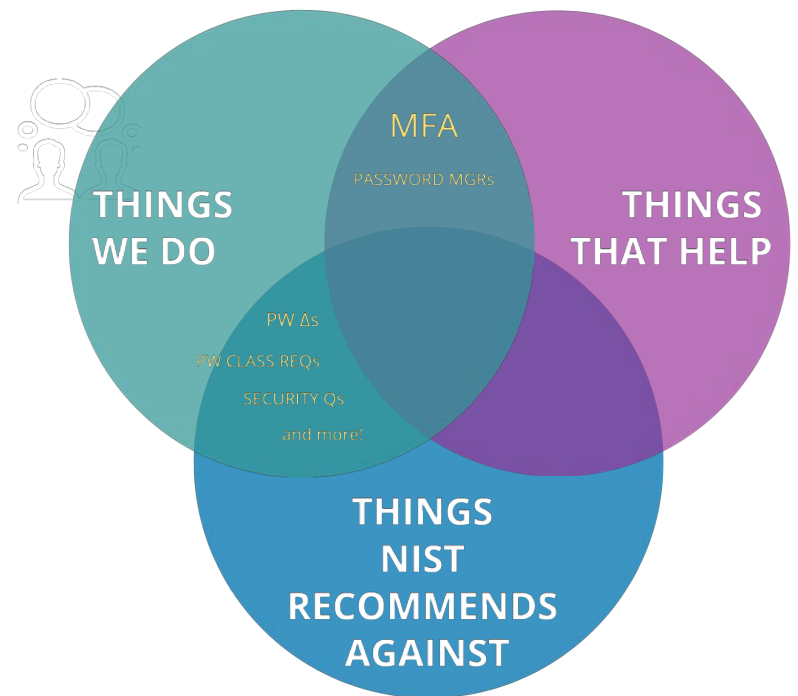
We'll do it with math!

“

- 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



# "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

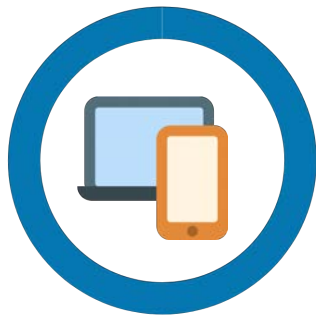


Device Attestation  
(vendor, model, features)



Device Filtering/Selection  
(what will you accept?)

# Wait, how is this multi-factor?



something you have  
[registered device]



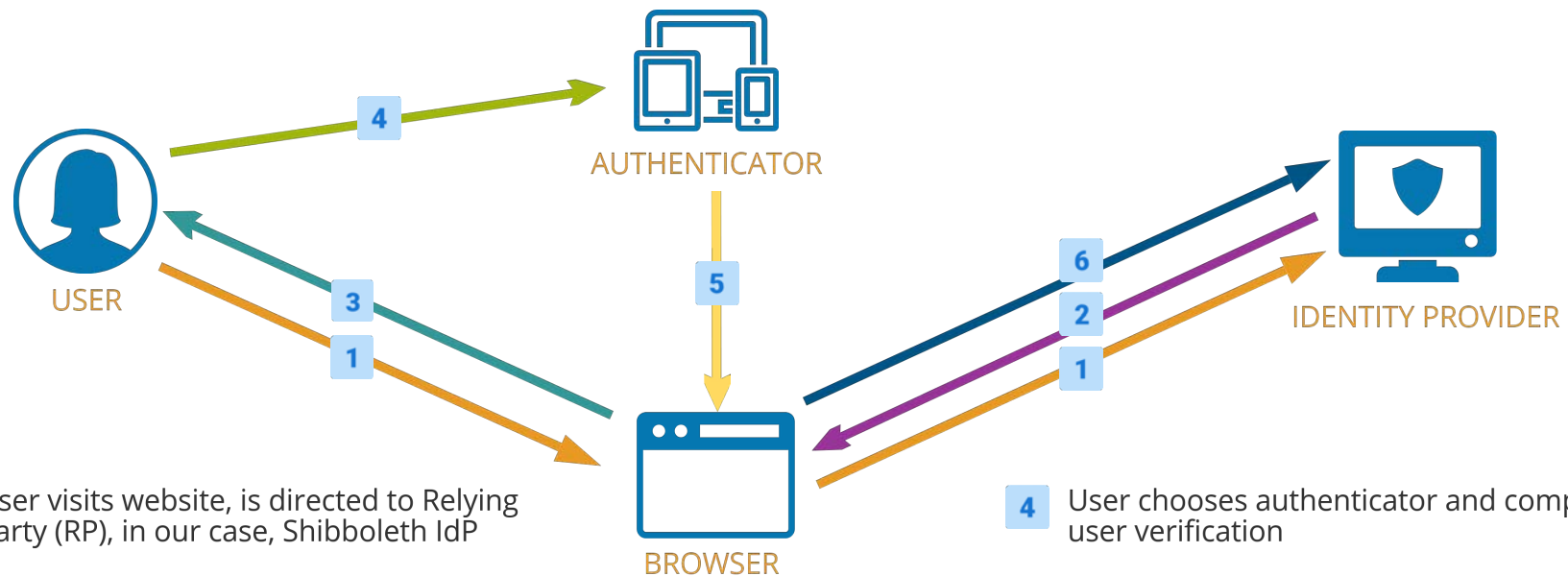
something you are  
[fingerprint, facial recognition]



something you know  
[PIN, gesture]

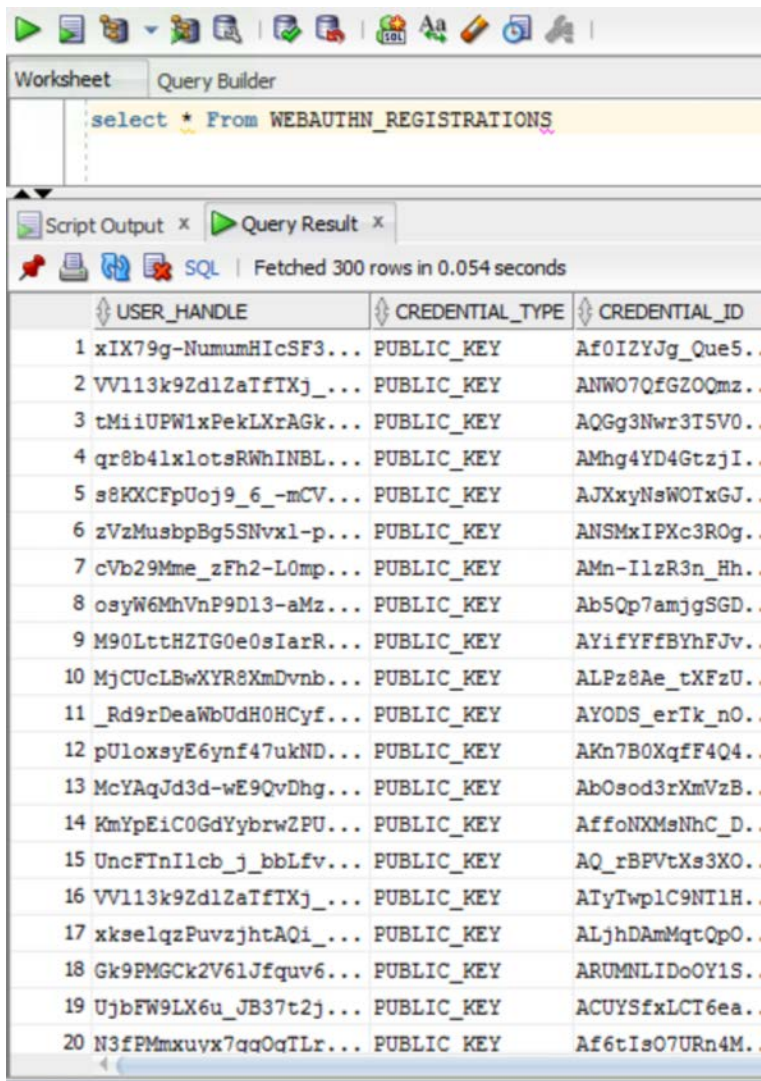
Uneasy with biometrics? Great! **Don't use them.**  
How you achieve MFA is between you and your device.

# 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

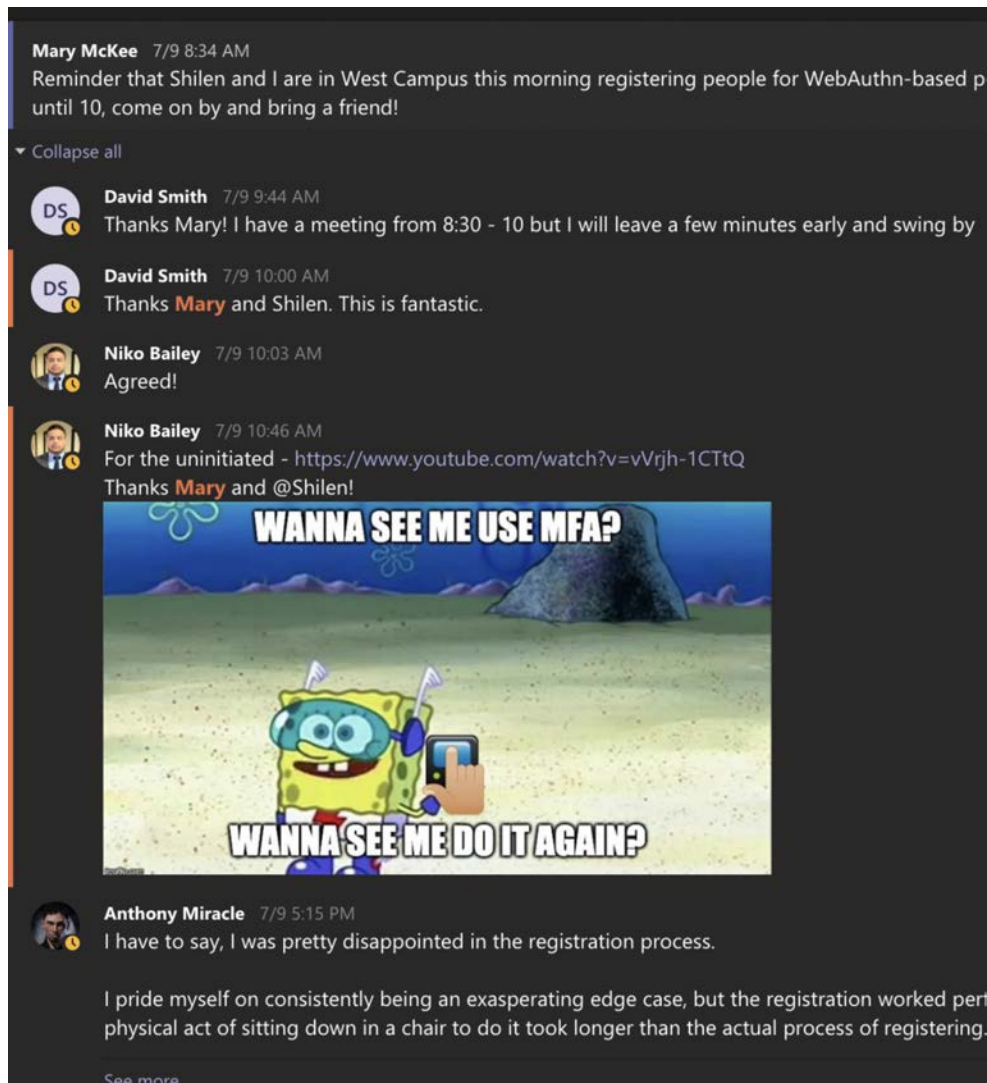


The screenshot shows a database query builder interface. At the top, there's a toolbar with various icons. Below it, a 'Worksheet' tab is active, displaying a SQL query: `select * From WEBAUTHN_REGISTRATIONS`. Below the query, there's a 'Script Output' and 'Query Result' section. The 'Query Result' section shows a table with 300 rows fetched in 0.054 seconds. The table has three columns: `USER_HANDLE`, `CREDENTIAL_TYPE`, and `CREDENTIAL_ID`. The first 20 rows are displayed, showing various user handles, all with a `PUBLIC_KEY` credential type, and their corresponding credential IDs.

	USER_HANDLE	CREDENTIAL_TYPE	CREDENTIAL_ID
1	xIX79g-NumumHicSF3...	PUBLIC_KEY	Af0IZYJg_Que5..
2	VV113k9Zdl2aTfTXj_...	PUBLIC_KEY	ANW07QfGZOQmz..
3	tMiiUPW1xPekLXrAGk...	PUBLIC_KEY	AQGg3Nwr3ISV0..
4	qr8b41xlotsRWhINBL...	PUBLIC_KEY	AMhg4YD4GtzjI..
5	s8KXCfpUoj9_6_-mCV...	PUBLIC_KEY	AJXxyNsWOTxGJ..
6	zVzMusbpBg5SNvx1-p...	PUBLIC_KEY	ANSMxIPXc3ROg..
7	cVb29Mme_zFh2-L0mp...	PUBLIC_KEY	AMn-IlzR3n_Hh..
8	osyW6MhVnP9D13-aMz...	PUBLIC_KEY	Ab5Qp7amjgSGD..
9	M90LttHZIG0e0sIarR...	PUBLIC_KEY	AYifYfFbYhFJv..
10	MjCUcLBwXYR8XmDvnb...	PUBLIC_KEY	ALPz8Ae_tXFzU..
11	_Rd9rDeaWbUdH0HCyf...	PUBLIC_KEY	AYODS_erTk_n0..
12	pUloxsyE6ynf47ukND...	PUBLIC_KEY	AKn7B0XqfF4Q4..
13	McYAqJd3d-wE9QvDhg...	PUBLIC_KEY	Ab0sod3rXmVzB..
14	KmYpEiC0GdYybrwZPU...	PUBLIC_KEY	AffonXMsNhC_D..
15	UncFTnIlcb_j_bbLfv...	PUBLIC_KEY	AQ_rBPVtXs3XO..
16	VV113k9Zdl2aTfTXj_...	PUBLIC_KEY	ATyTwplC9Nt1H..
17	xkselqzPuvzjhtAQi_...	PUBLIC_KEY	ALjhDAMqtQpO..
18	Gk9PMGCK2V61Jfquv6...	PUBLIC_KEY	ARUMNLIDoOY1S..
19	UjbFW9LX6u_JB37t2j...	PUBLIC_KEY	ACUYSfxLCT6ea..
20	N3fPMmxuyx7qqOaTLr...	PUBLIC_KEY	Af6tIsO7URn4M..

# 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.

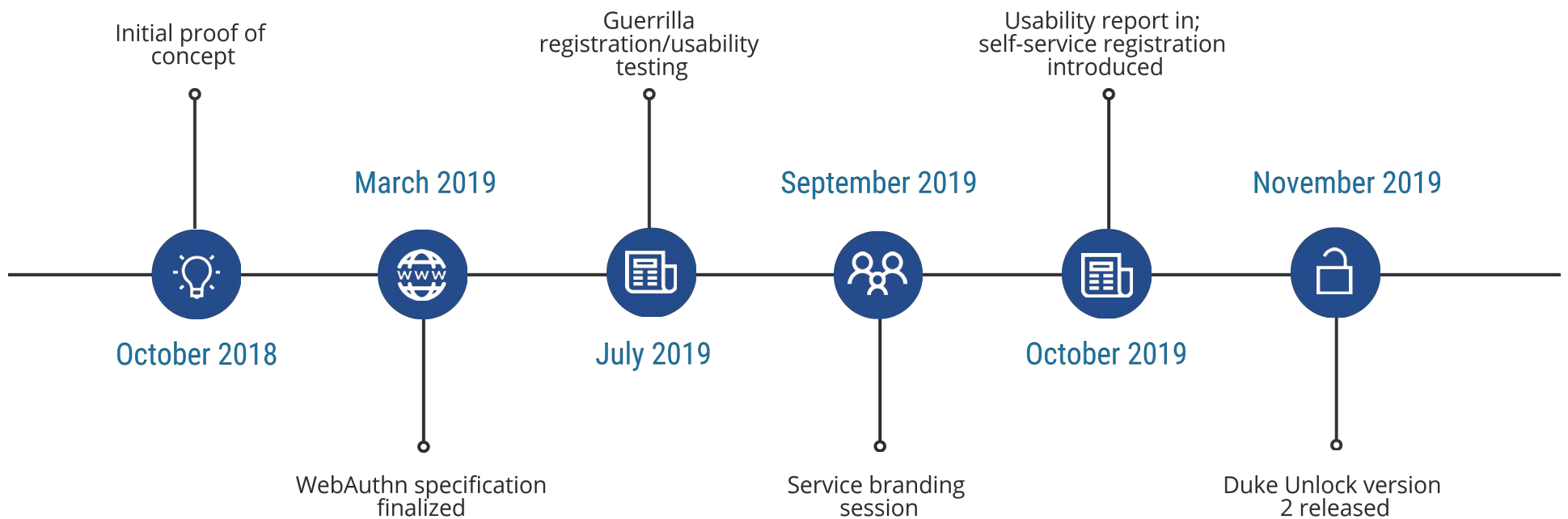
## NEXT: Actual usability tests

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





# HOW

We deployed Duke Unlock.

# Duke **Unlock** - Service Values

SECURITY	COMMUNITY	THRIFT	PROGRESS
<ul style="list-style-type: none"><li>• Expand coverage of MFA.</li><li>• Increase user engagement on account security.</li></ul>	<ul style="list-style-type: none"><li>• Listen to feedback and frustrations.</li><li>• Measure word-of-mouth referrals to gauge success.</li></ul>	<ul style="list-style-type: none"><li>• Only invest in what people are responding to.</li><li>• Scale MFA use without scaling MFA cost.</li><li>• Don't ask users to increase \$/time investment (BYO-MFA).</li></ul>	<ul style="list-style-type: none"><li>• Skate to where the puck is going.</li><li>• Embrace quickly changing tech landscape.</li><li>• Engineer for tomorrow.</li></ul>

# Duke Log In

You are on the correct Duke login page if the above begin

## NetID

Current students, faculty, staff, sponsored guests

NetID

Password

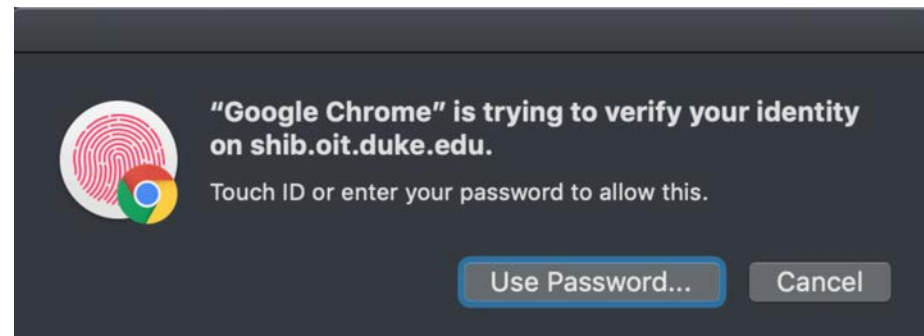
[Forgot your password?](#)

[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



# Duke Log In

You are on the correct Duke login page if the above begins with: <https://shib.oit.duke.edu>

NetID

Current session

Device Support

Browser Support

User Grasp

NetID

mkm16

Passwordless Login

Your device  
tap your  
device.

User Engagement

Ease of Registration

Remember to Use

You will be logged in automatically.

Can't complete this step? [Go back](#)



"Google Chrome" is trying to verify your identity on shib.oit.duke.edu.

Touch ID or enter your password to allow this.

*Known Issues with v1*

# Duke Log In

You are on the correct Duke login page if the above begins with: <https://shib.oit.duke.edu>

NetID

Current status

Device Support

Browser Support

User Grasp

NetID

mkm16

Passwordless Login

Your device  
tap your  
device.

User Engagement

Ease of Registration

Remember to Use

You will be logged in automatically.

Can't complete this step? [Go back](#)



"Google Chrome" is trying to verify your identity on shib.oit.duke.edu.

Touch ID or enter your password to allow this.

*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

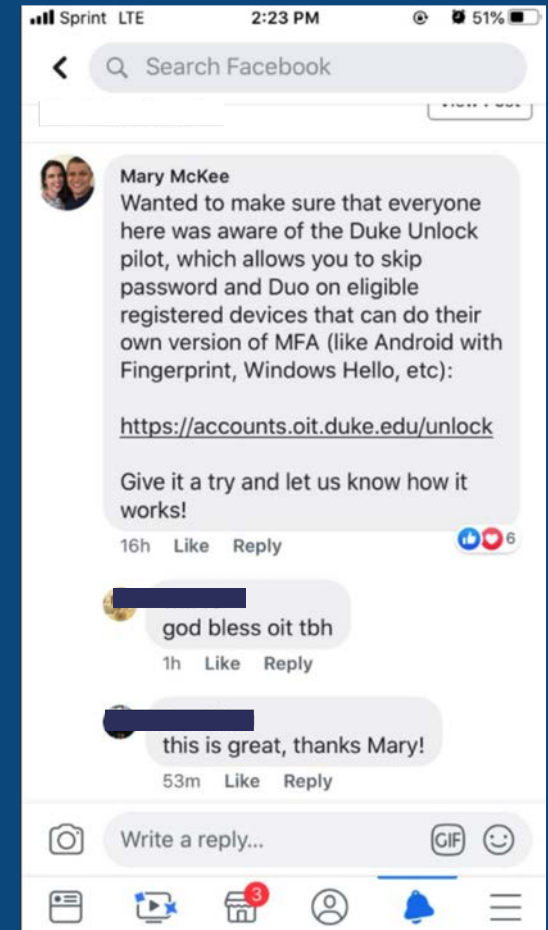
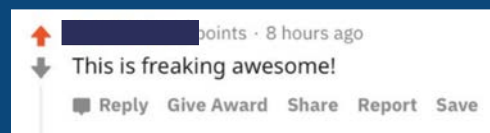


## PROBLEM: USER ENGAGEMENT

# 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?**



### Summary

I conducted individual, moderated user testing sessions and follow up interviews with the objective of evaluating both the registration experience and daily user experience of OIT's passwordless authentication pilot. All participants were asked how they learned about the pilot and what they knew going into it. Those already registered were asked for feedback on their experience using WebAuthn (Duke Unlock). Registration usability testing was conducted with those not yet registered or who wanted to register an additional device. Brief follow up interviews were later conducted with those who registered with me. Feedback passed on to me via email was also logged.

**Participants:** I collected feedback from 22 people. Nine of these were already registered and had been using the service. Fifteen people registered either for the first time or registered an additional device.

- 10 people registered a Macbook Pro with Chrome
- 8 people registered an Android with Chrome
- 5 people registered a PC with Chrome, Edge, Brave, or Firefox

### Key Findings and Recommendations

- Participants were positive, even frequently enthusiastic about using Duke Unlock.
- The registration email appeared to some participants to be written for a technical audience. Making registration more straightforward for non-technical users is advised. Simplify the wording (whether in an email or on a webpage).
- Enable users to set Duke Unlock as their default authentication mechanism for that device and browser so they can avoid having to click a link each time they log in.
- Change the location and wording of the "Go Passwordless" link (if the link is necessary)
- If possible, do not show the Duke Unlock option on devices/browsers that do not support it (likely not a viable option until the technology stabilizes).
- Create a self-service experience where users can update device nicknames, register additional devices, remove registered devices and set their device default to use Unlock.
- Provide some up-front onboarding and re-onboard as necessary so users know to re-register when they clear cookies from a registered device.
- Improve mobile layout

## PROBLEM: EASE OF REGISTRATION

# Usability Research

## USER FEEDBACK:

"It just...works!"

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

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

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

"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.

## PROBLEM: REMEMBERING TO USE

# 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

## NetID

Current students, faculty, staff, sponsored guests

NetID

bdevil123

Password

[Forgot your password?](#)

[Use Duke Unlock to go passwordless](#)

Log In

Make link part of  
on-boarding



## NetID

Current students, faculty, staff, sponsored guests

NetID

bdevil123

Log in with Duke Unlock

☒ **Make Duke Unlock the default for this browser on this device**

Your browser will now prompt you to complete login with your registered device.

Can't complete this step? [Go back](#)

# Duke Log In

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](https://oit.duke.edu/help) or [dhts.duke.edu](https://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.

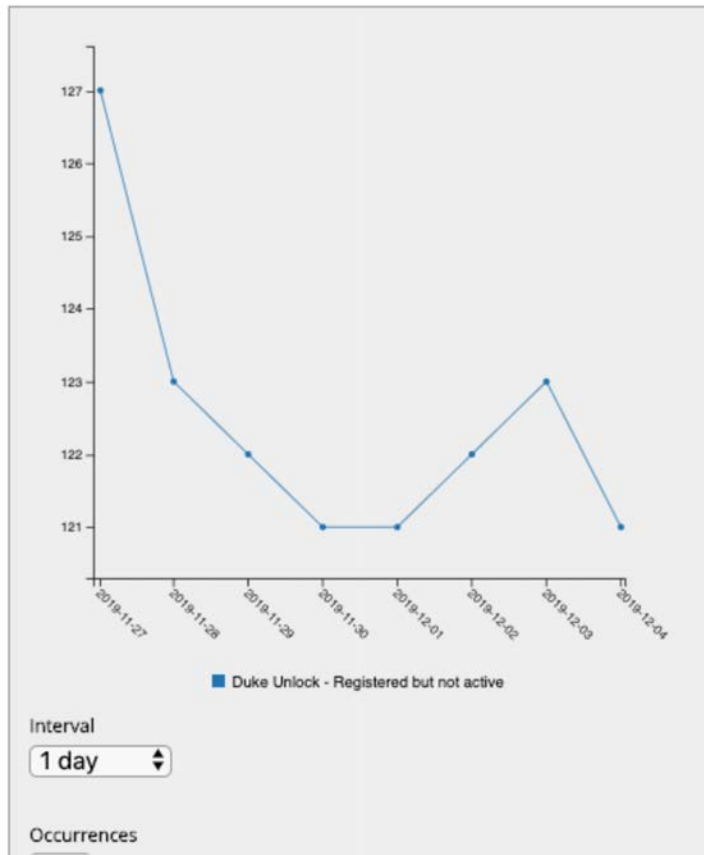


# FUTURE

Scaling up and out.

[flag](#) > [authentication](#) > [unlock-registered-not-active](#)

## Membership Graph: Duke Unlock - Registered but not active



# 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

01

## 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.

## SOUNDS

## FEELINGS/SENSES

Thank You!



Questions?

UFO!  
beam me  
up, Scotty!

Key in lock

Phone unlock  
click

Step on  
the stairs  
(personal  
gro)

Checked  
baggage  
vs  
error

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Like  
someone  
saying

Easy  
key

You  
connect

Quick  
click

Unlock

Quick  
connect

Fastenings

Fastenings

Fastenings

Fastenings

Fastenings

Fastenings

Fastenings

Fastenings

Fastenings

Fastenings

Fastenings

ominous  
tones

gong

bell  
"ding-dong"

chime

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

unlock  
"whoosh"

cup/mug

ding

light sabre

"Success"

"Success"

"Success"

"Success"

"Success"

"Success"

"Success"

"Success"

"Success"

"Success"

"Success"

"Success"

"Success"

joyous  
choir

"creeeen"  
K

"bing!"

12 notes

12 notes

12 notes

12 notes

12 notes

12 notes

12 notes

12 notes

12 notes

12 notes

12 notes

12 notes

12 notes

Satisfaction

Productive

Winning  
(ambitious/  
early work)

Pop!  
(unlock or  
button press)

Validation

Cool

Freedom

Touch

reveal  
the answer  
to a mystery

No feelings  
at all  
because  
so easy/quick