


Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.



Widely Reused and Shared, Infrequently Updated, and Sometimes Inherited: A Holistic View of PIN Authentication in Digital Lives and Beyond

Hassan Khan, **Jason Ceci***, Jonah Stegman
University of Guelph

Adam J. Aviv
The George Washington University

Rozita Dara
University of Guelph

Ravi Kuber
University of Maryland,
Baltimore County

PINs



[Source: thebalance.com]

PINs

- Many mobile and web apps switching to PIN-based authentication as the default option
- Many loyalty cards now require PINs
- Most keyless home locks use PIN authentication

Background

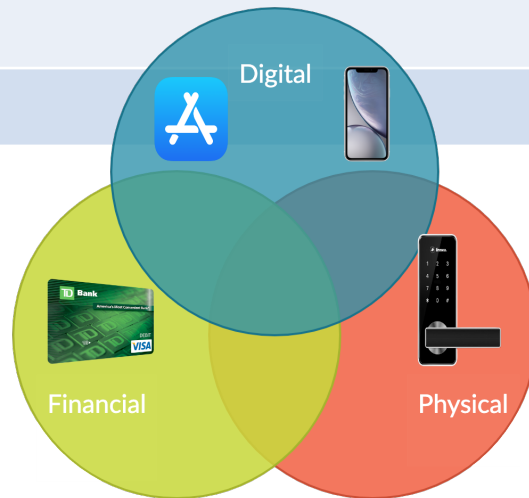
- Previous studies have investigated the guessability of human-chosen PINs.¹ However, the factors influencing PIN selection have not been investigated.
- A range of studies have focused on defending against attacks on PINs.²
- There is little research into users' reported frequency of these attacks, the defenses employed in different contexts and the recourse of users after an attack

1. Bonneau et al. "A birthday present every eleven wallets? The security of customer-chosen banking pins." International Conference on Financial Cryptography and Data Security 2012

2. Aviv et al. "Towards baselines for shoulder surfing on mobile authentication" ACSAC 2017

Categorizing PINs

Digital	Financial	Physical
Smartphones	ATM	Garage Door
Tablets	Debit Cards	Home Lock
Laptop or Desktop Computers	Credit Cards	Smart Locks
Smart Watches	Loyalty/reward cards	Thermostats
Apps	Online Banking	Smart Home Devices
Websites / Online Accounts		Bike Locks
Netflix / Video on Demand		Car Locks
Gaming Consoles		Padlocks
Voicemail		Garage Door



Research Questions

A broad analysis of PIN usage to determine how individuals use PINs across a wide variety of assets.

1. How do individuals select new PINs? When do individuals update their PINs?
2. How often do users perceive attacks on their PINs in the wild?
3. Who do individuals share their PINs with, and how does this vary with asset type?

We conduct semi-structured interviews with 35 participants to answer these question

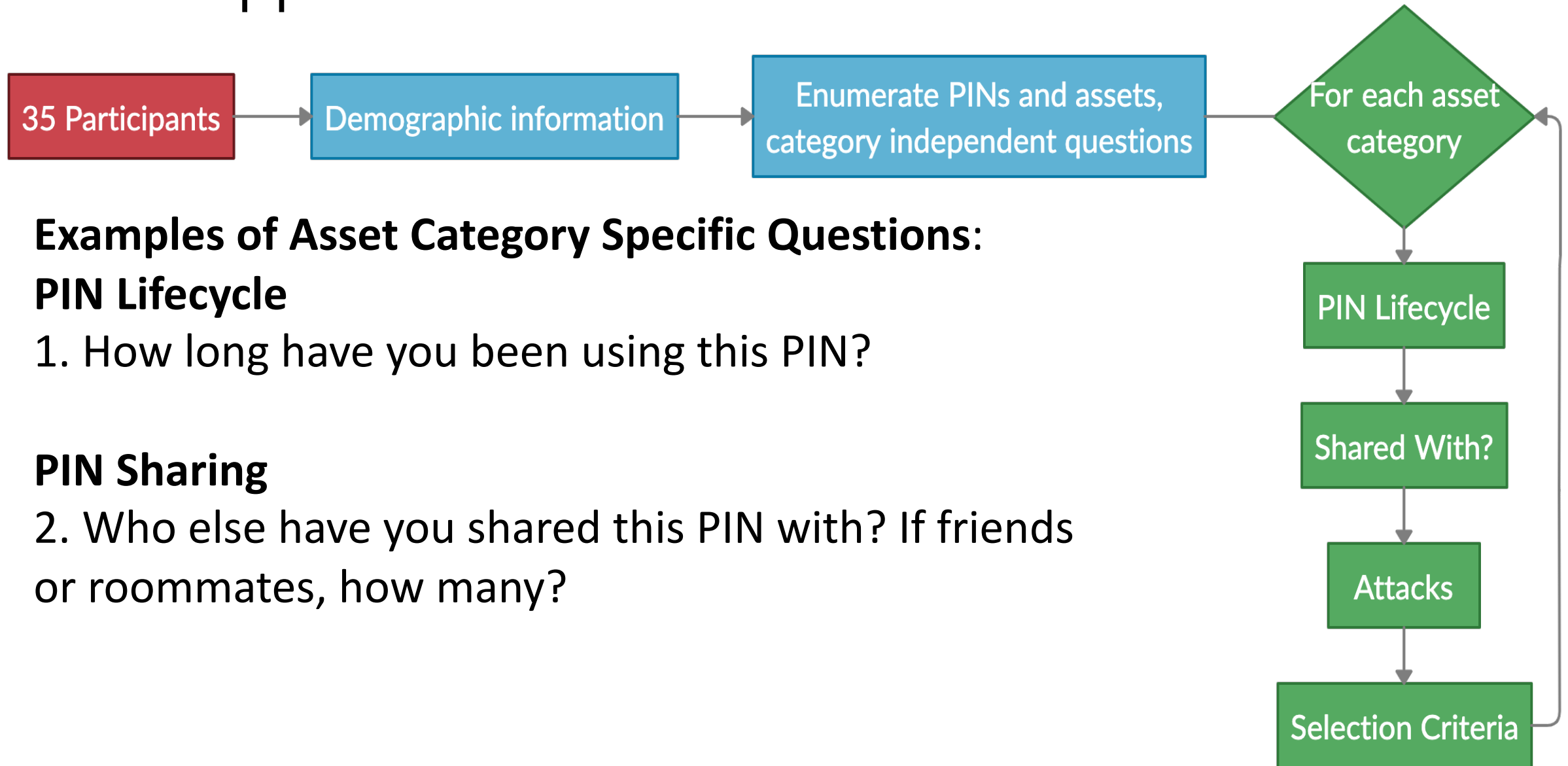
The Participants

Table 1: Participants' demographics (* UD = Undisclosed)

n = 35							
Gender							
Female				Male			
17				18			
Age (in years)							
18–25	26–30	31–35	36–40	41–45	46–50	50+	
8	4	5	6	6	1	5	
Annual Household Income (× \$1000)							
>\$15	\$15–29	\$30–49	\$50–74	\$75–99	\$100–150	>\$150	UD*
2	2	3	4	5	10	2	7
Highest Education Level							
High School			Undergraduate			Graduate	
17			6			12	
Self Reported Proficiency in Technology							
Basic			Intermediate			Advanced	
6			18			11	
Self Reported Proficiency in Security							
Basic			Intermediate			Advanced	
19			9			7	

The interviews were conducted on a well-balanced participant pool.

Our Approach



Examples of Asset Category Specific Questions:

PIN Lifecycle

1. How long have you been using this PIN?

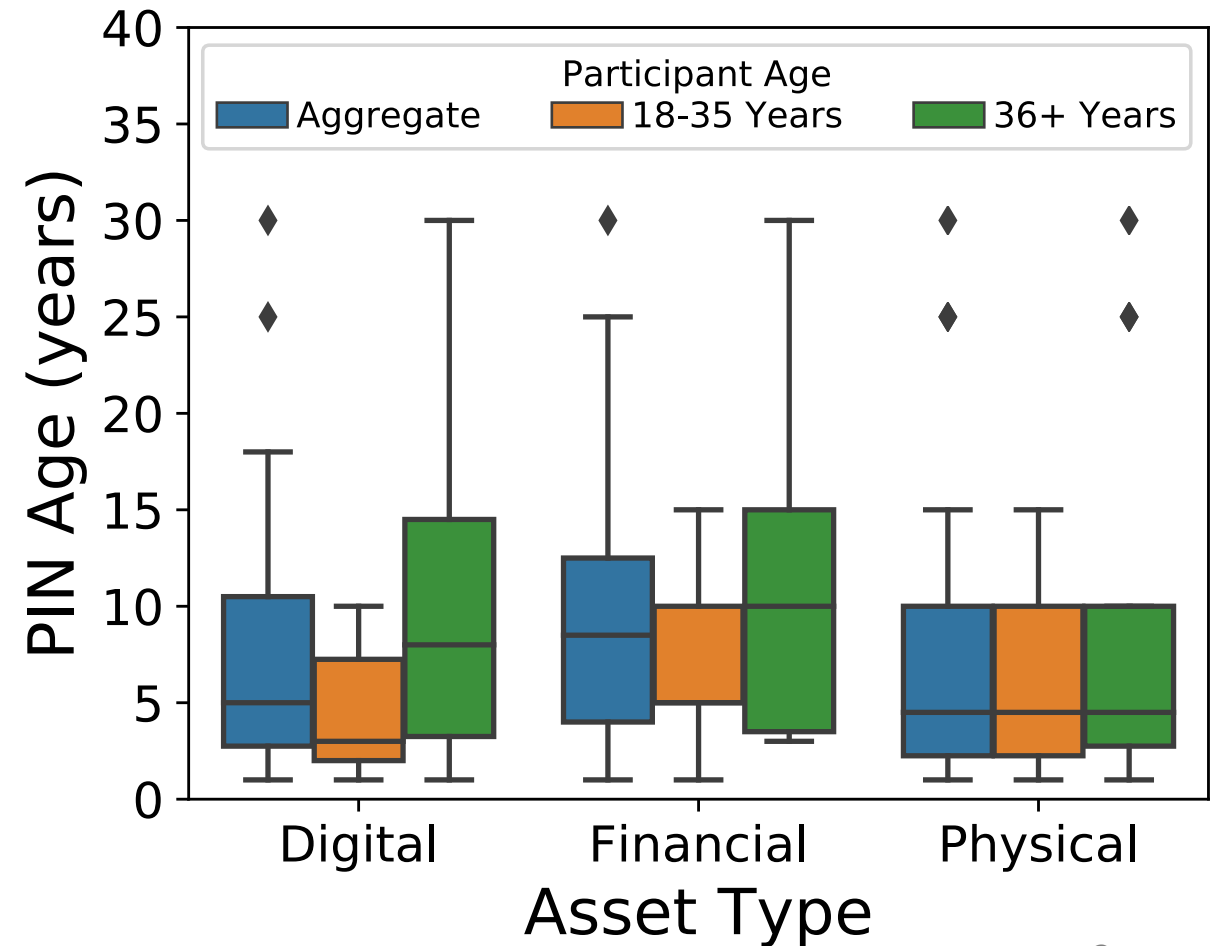
PIN Sharing

2. Who else have you shared this PIN with? If friends or roommates, how many?

PIN Age

There was no evidence to suggest that PIN age varied significantly between asset types.

Total	Per Participant		
PINs	Minimum	Maximum	Average
140	1	15	4

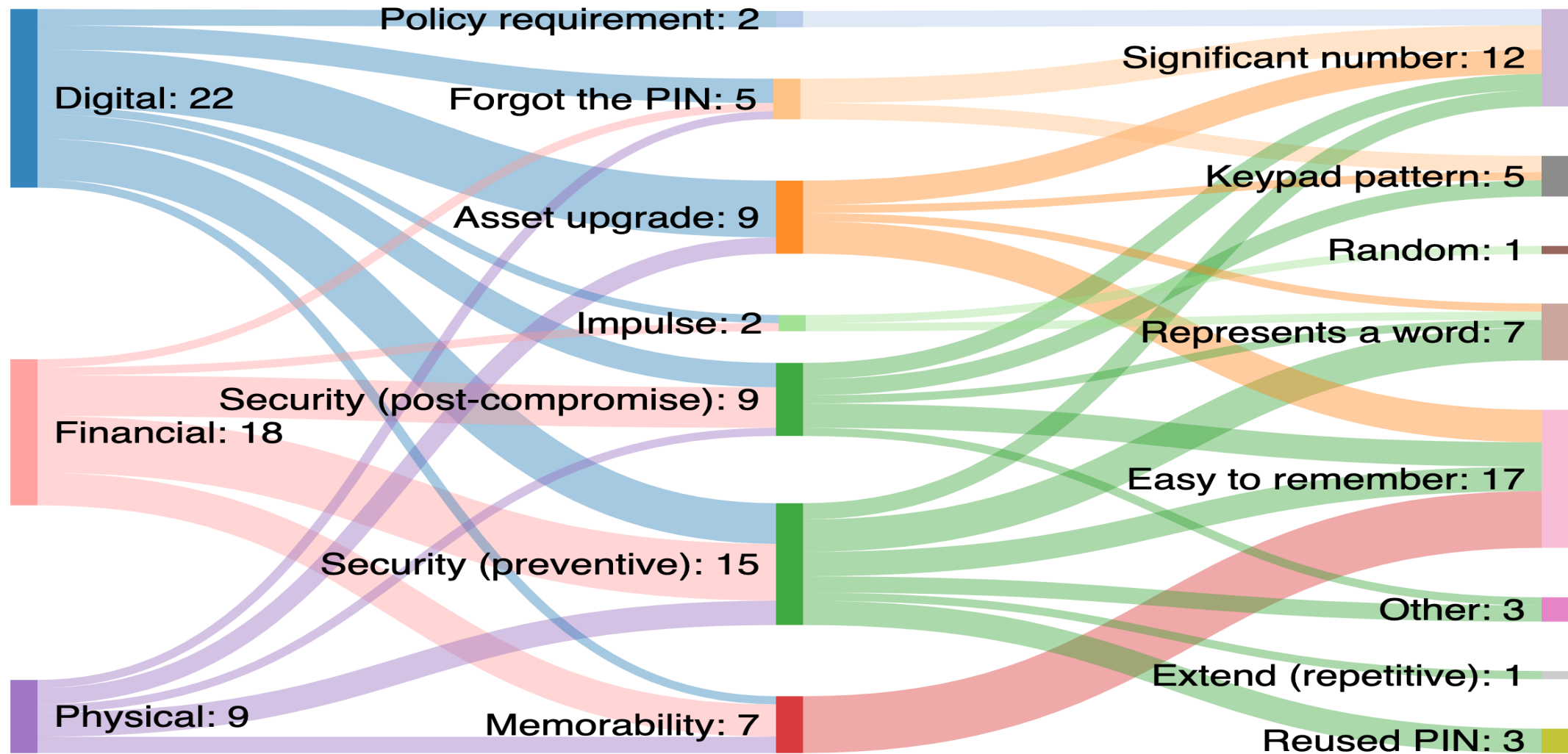


PIN Choices

- We investigate the factors that motivate PIN choices.
- For each asset type, participants were asked to rank the importance of four criteria when choosing PINs for that asset type:
 - Security (Choosing a PIN that will best protect the asset)
 - Memorability (Choosing a PIN that is easy to remember)
 - Usability (Choosing a PIN that is easy to enter)
 - Reusability (Choosing a PIN that I currently use for another item)
- Average ranks: Memorability > Security > Usability > Reusability

Participants ranked memorability as most important and reusability as the least important factor when choosing PINs but widely reused PINs.

PIN Updates



Regardless of the reasons behind updating their PIN, many users chose insecure PIN selection strategies.

PIN Sharing

<i>Shared with</i>	<i>Digital</i> (<i>n=32</i>)	<i>Financial</i> (<i>n=34</i>)	<i>Physical</i> (<i>n=27</i>)
None	6	7	1
Spouse	16	17	13
Children	9	6	8
Parents	3	7	10
Siblings	5	2	5
Girl/Boyfriend	5	3	4
Friends	5	2	9
Helpers	0	0	8

We found widespread PIN sharing across different relationship types.

PIN Reuse

Table 6: Reported reuse of PINs

Have you reused PINs?

No: 7/35 (20%)

Yes: 28/35 (80%)

Type of reuse

18/28 across all asset types

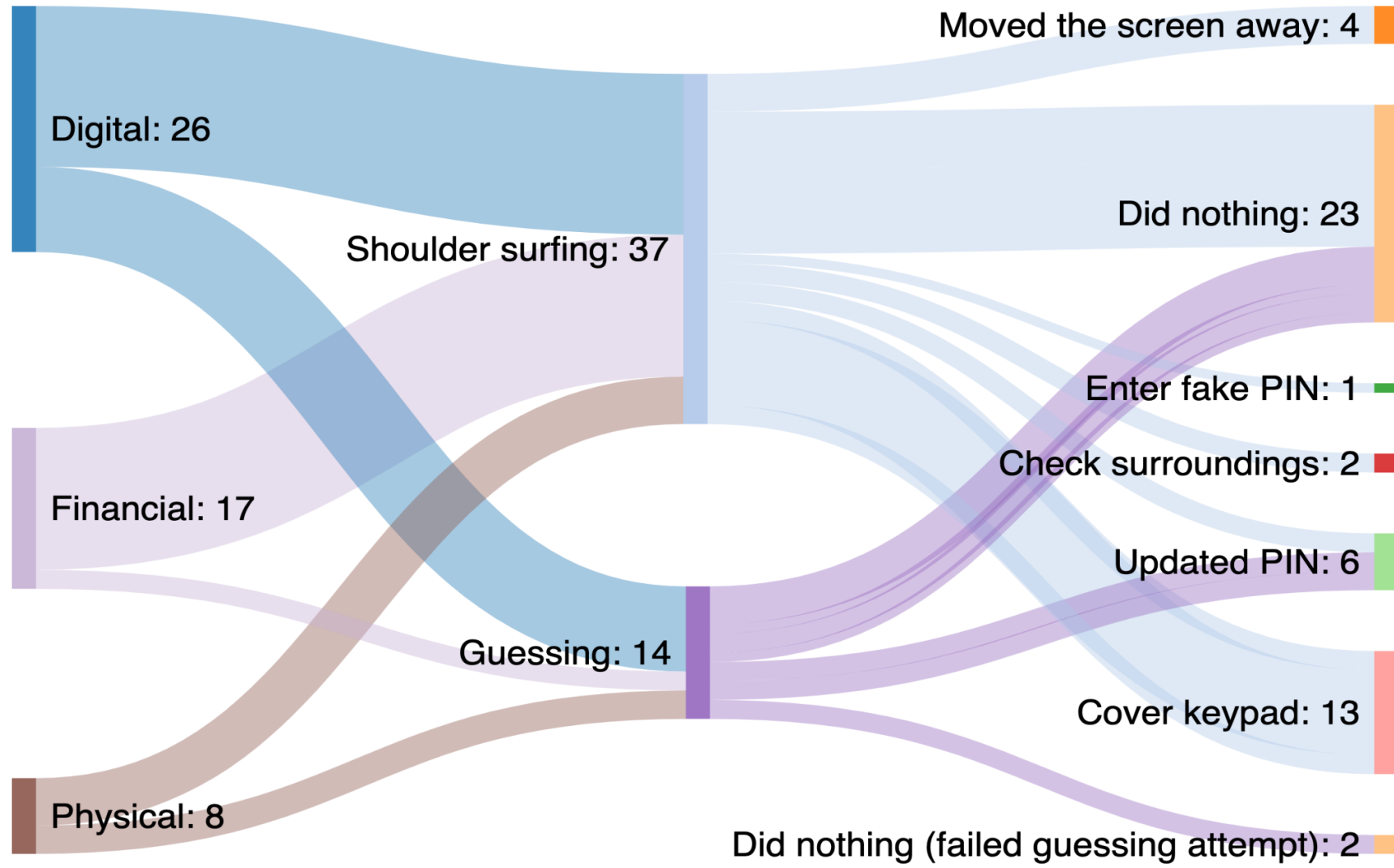
3/28 same asset type only

4/28 across digital and physical

3/28 across digital and financial

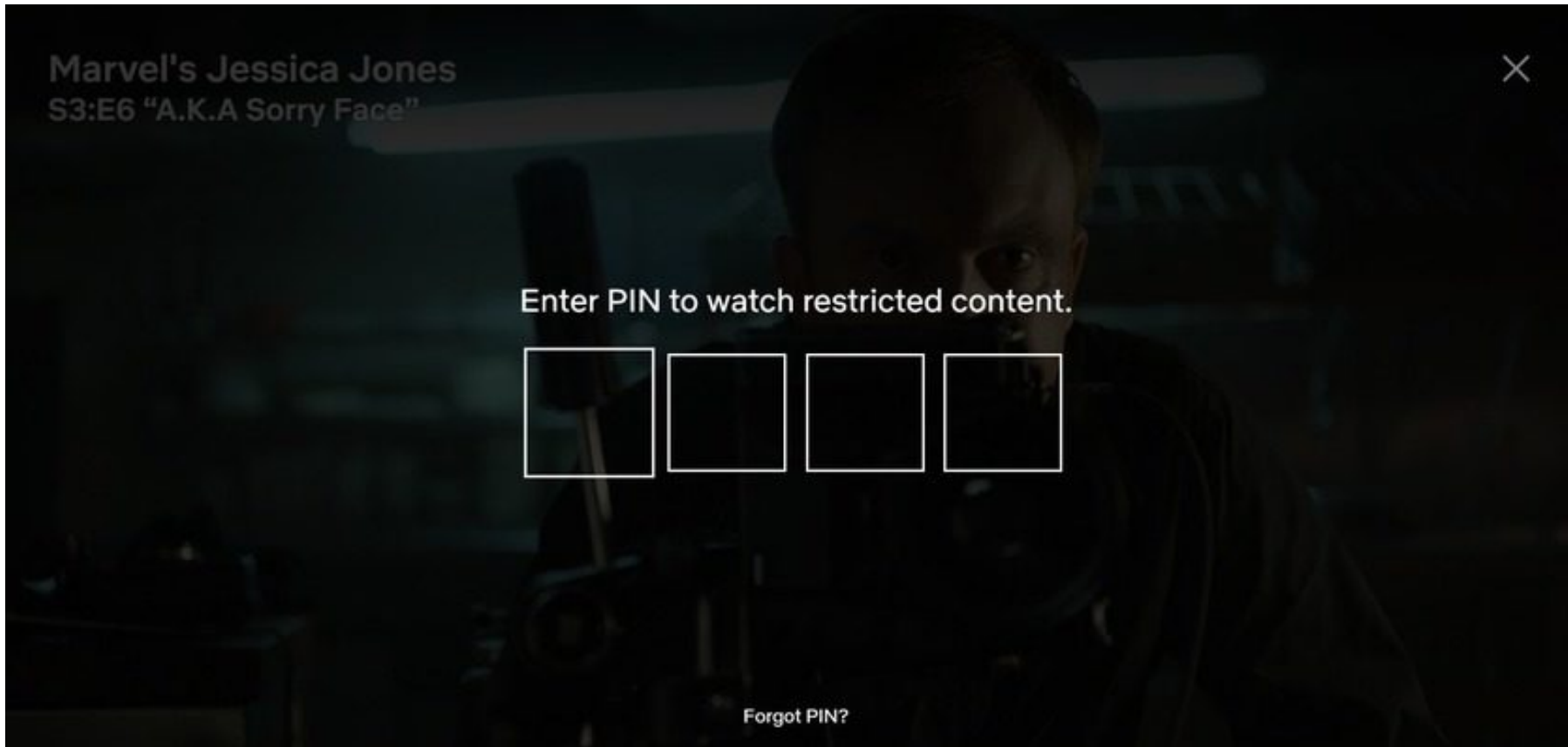
Most participants reused PINs, and many reused PINs across asset types.

Attacks on PINs



Many participants reported taking no action in response to shoulder surfing or guessing attacks.

PIN Interfaces



Issues with PIN interfaces and update mechanisms reduce the usability and security of PIN authentication.

Widely Reused and Shared, Infrequently Updated, and Sometimes Inherited: A Holistic View of PIN Authentication in Digital Lives and Beyond

- Our findings show widespread sharing and reuse of PINs for memorability reasons
- Participants voiced a lack of confidence in PIN authentication due to the ease and frequency of shoulder surfing attacks
- PIN management behaviours differed between asset types due to the availability of recourse in case of compromise

Thank You

Hassan Khan
(hassan.khan@uoguelph.ca)

Jason Ceci*
(jceci@uoguelph.ca)

Jonah Stegman
(jstegman@uoguelph.ca)

Adam J. Aviv
(aaviv@gwu.edu)

Rozita Dara
(drozita@uoguelph.ca)

Ravi Kuber
(rkuber@umbc.edu)

UNIVERSITY
of GUELPH

THE GEORGE
WASHINGTON
UNIVERSITY

WASHINGTON, DC

UNIVERSITY
of GUELPH



UMBC