



# This PIN Can Be Easily Guessed

Analyzing the Security of Smartphone Unlock PINs

Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv

RUHR  
UNIVERSITÄT  
BOCHUM

RUB

Max Planck Institute  
for Security and Privacy



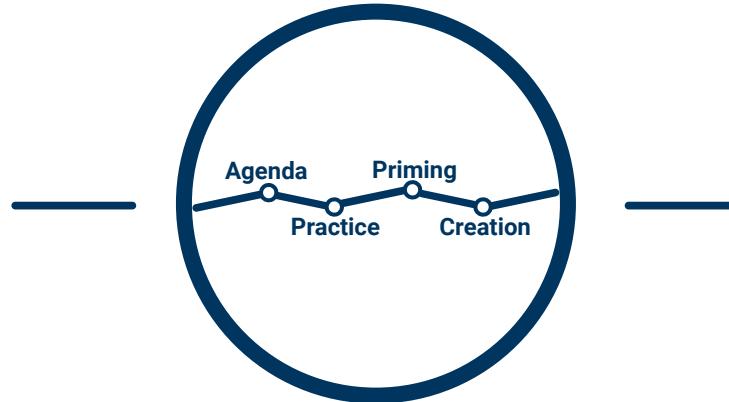
THE GEORGE  
WASHINGTON  
UNIVERSITY  
WASHINGTON, DC

GW

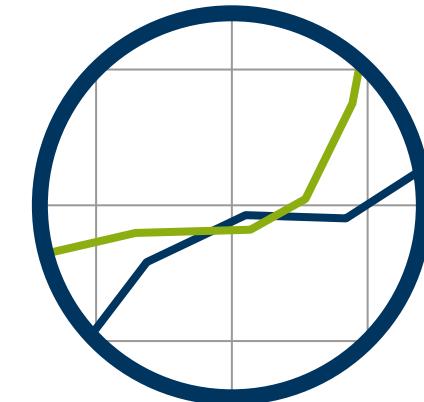
# Overview



Why study PINs?



User Study

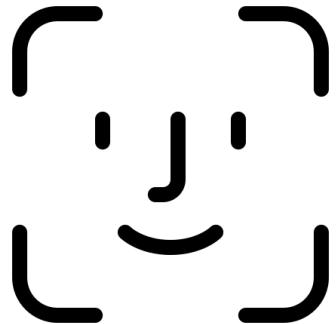


Results

# Why PINs?



Fingerprint



Face



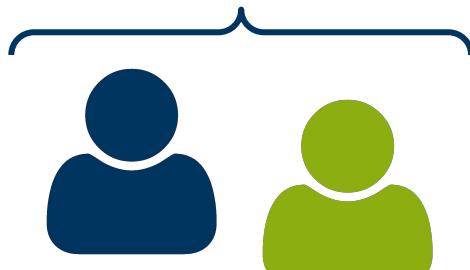
PHOTO: Dan Seifert | The Verge (Vox Media)

Iris

# Who uses PINs?

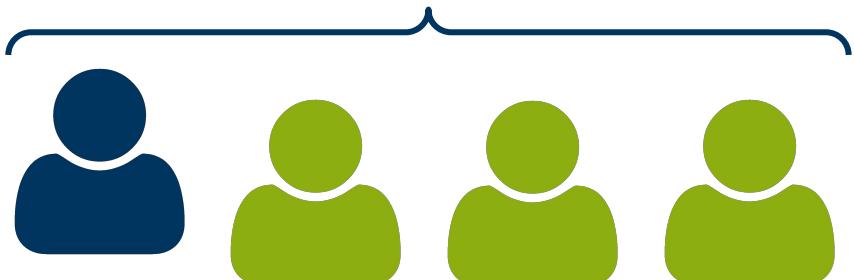
**1220 participants**

**461 do not use a biometric**



**210 use a PIN**

**759 use a biometric**



**595 use a PIN**

**Overall 805 (66%) use a PIN**

# What we know about PINs

- User chosen 4-digit PINs are predictable [1]
- User chosen 6-digit PINs aren't any better [2]
- Blocking popular PINs can increase security [1]

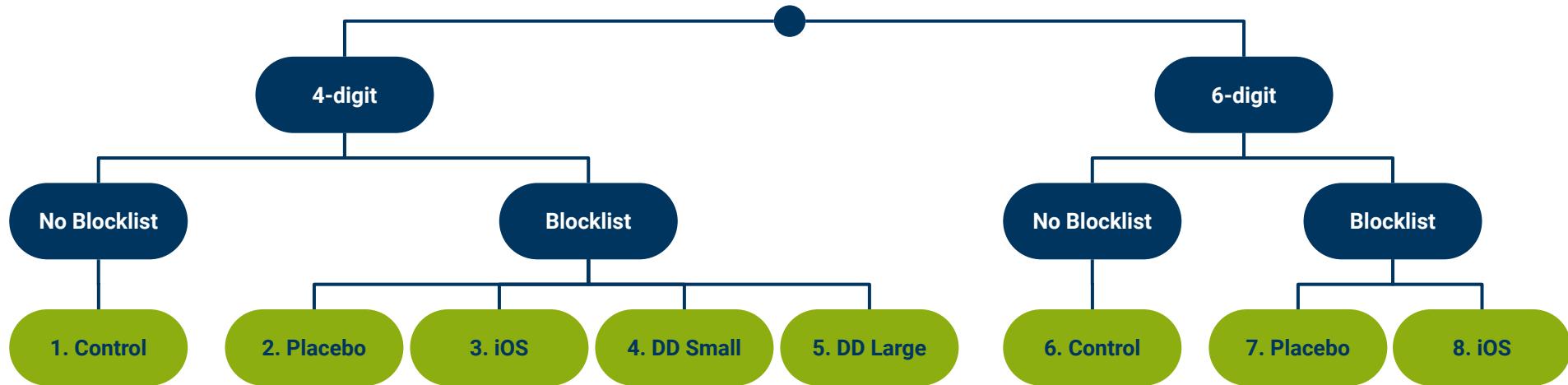
# What we don't know

- How secure are 4- or 6-digit PINs in the smartphone unlock setting?
- What are the effects of different blocklists on the security of PINs?
- How to balance security and usability when composing a blocklist?

[1] J. Bonneau, S. Preibusch, and R. Anderson. **A Birthday Present Every Eleven Wallets?** The Security of Customer-Chosen Banking PINs. FC '12

[2] D. Wang, Q. Gu, X. Huang, and P. Wang. **Understanding Human-Chosen PINs:** Characteristics, Distribution and Security. AsiaCCS '17

# Treatments



## Placebo

“Test general effect of warning”

Blocklist:

- “1st choice” blocked
- Any other PIN allowed

## iOS

“Test effect of iOS blocklists”

Blocklist:

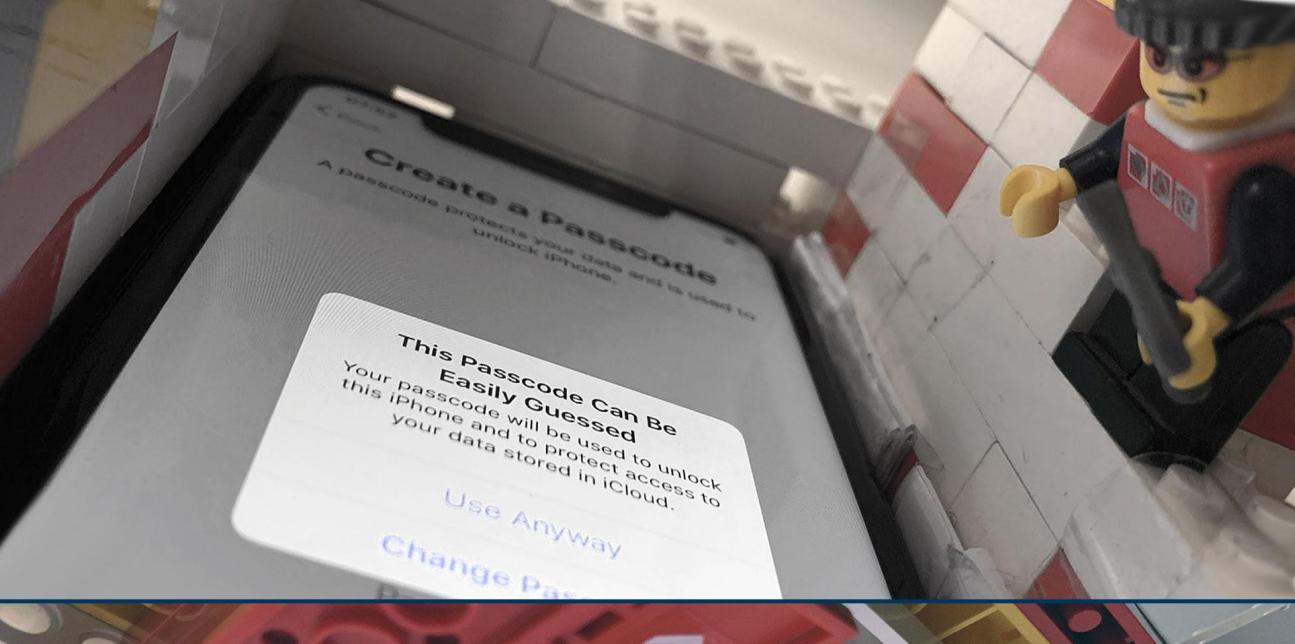
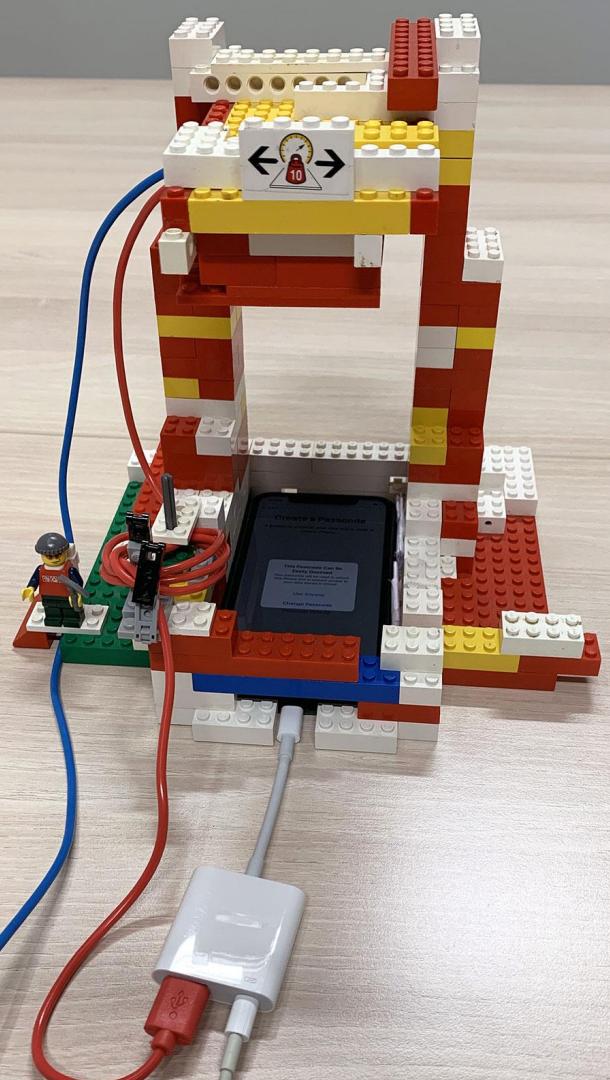
- 274 PINs (4-digit)
- 2910 PINs (6-digit)

## Data-Driven (DD)

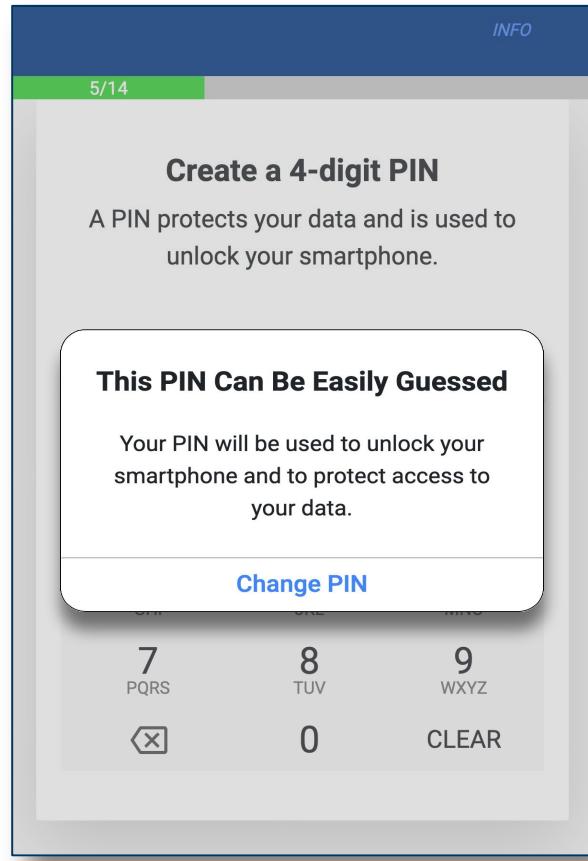
“Test effect of different blocklist sizes”

Blocklist:

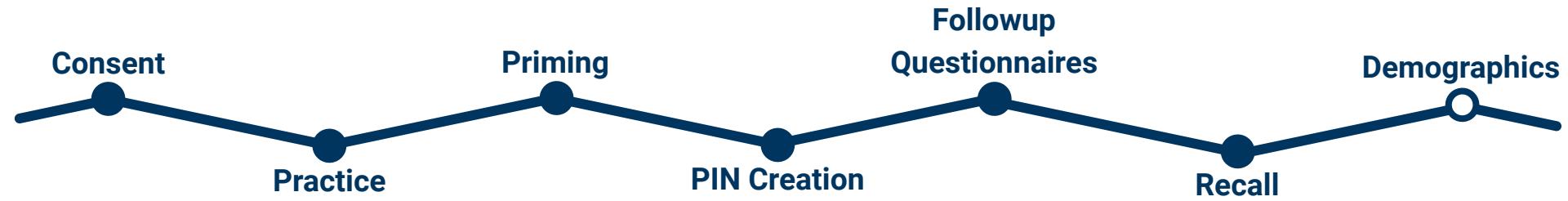
- Top 27 PINs of Amitay (small)
- Top 2740 PINs of Amitay (large)



# User Study



# User Study



# Attacker Model



- No information about the victim



# Attacker Model



- No information about the victim
- Guesses PINs in decreasing probability order

1 —  
2 —  
3 —

Rank	4-digit PINs	6-digit PINs
1	1234	123456
2	0000	123123
3	2580	111111
⋮	⋮	⋮

# Attacker Model



- No information about the victim



- Guesses PINs in decreasing probability order



- Slowed down by rate-limiting

You have incorrectly typed your PIN 5 times.

Try again in 30 seconds.

OK

Android	iOS
10 Guesses	30s    1h 36m 0s
100 Guesses	10h 45min 30s    —

# Attacker Model



- No information about the victim



- Guesses PINs in decreasing probability order



- Slowed down by rate-limiting



- Knows the blocklist and skips impossible choices

Rank	4-digit PINs	6-digit PINs
1	1234	123456
2	not allowed 0000	
3	2580	
⋮	⋮	

**This PIN Can Be Easily Guessed**

Your PIN will be used to unlock your smartphone and to protect access to your data.

[Change PIN](#)

# Research Questions

4 vs. 6

**RQ1:** How secure are 4- and 6-digit PINs in the smartphone unlock setting?

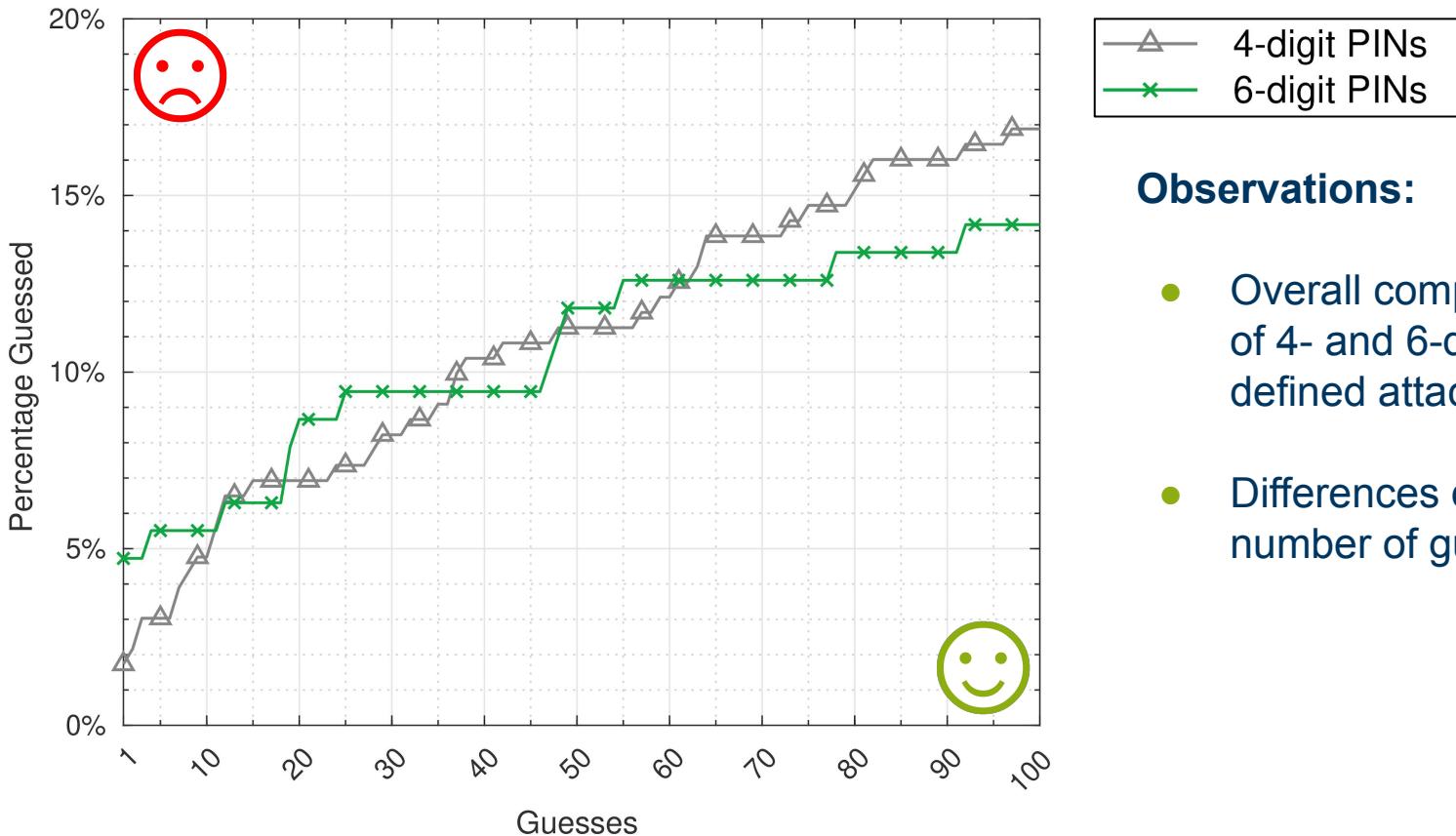
Small?  
Medium?  
Large?

**RQ2:** What are the effects of different blocklists on the security of PINs?



**RQ3:** How to balance security and usability when composing a blocklist?

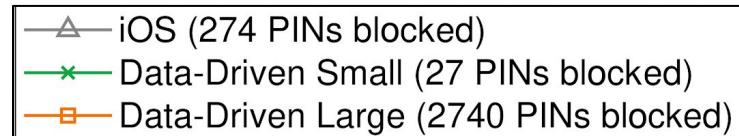
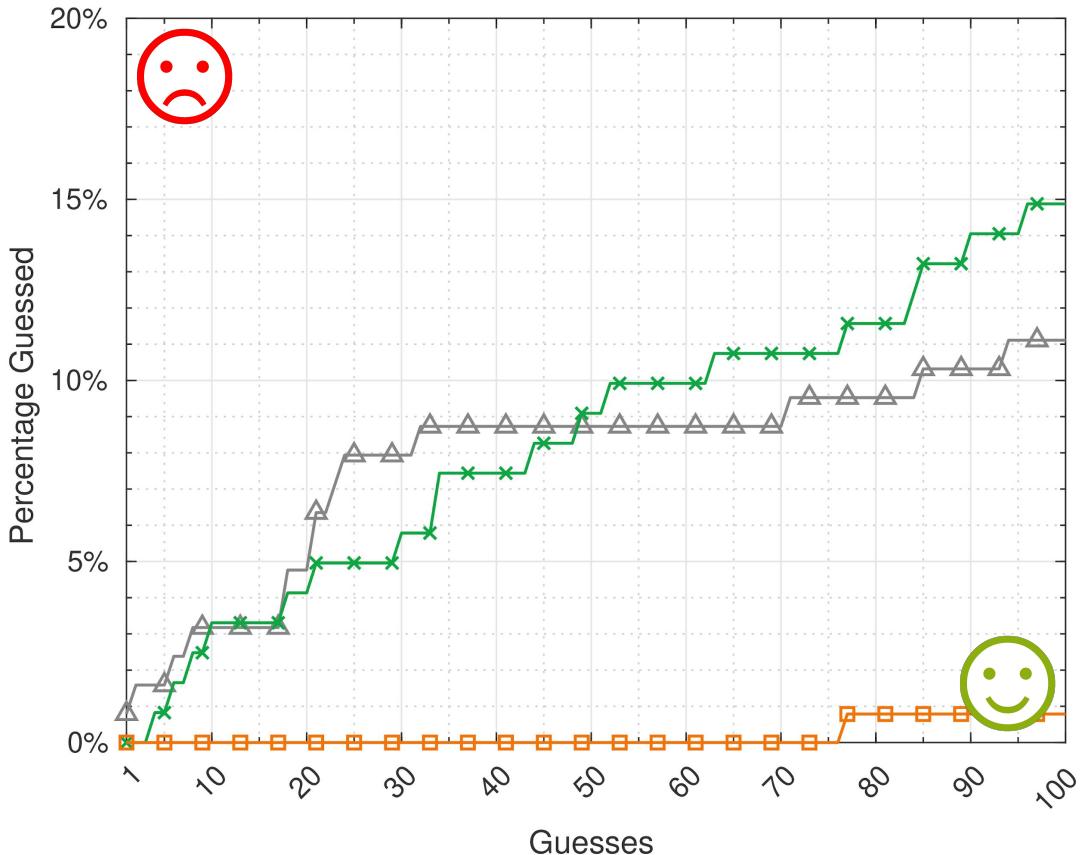
# RQ1: 4- vs. 6-digit PINs



## Observations:

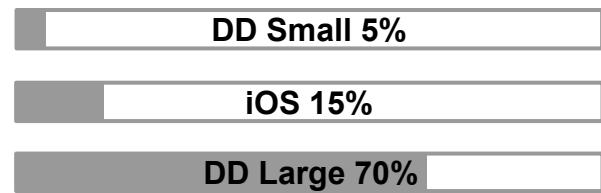
- Overall comparable security of 4- and 6-digit PINs in the defined attacker model
- Differences depending on the number of guesses

## RQ2: Different Blocklist Sizes

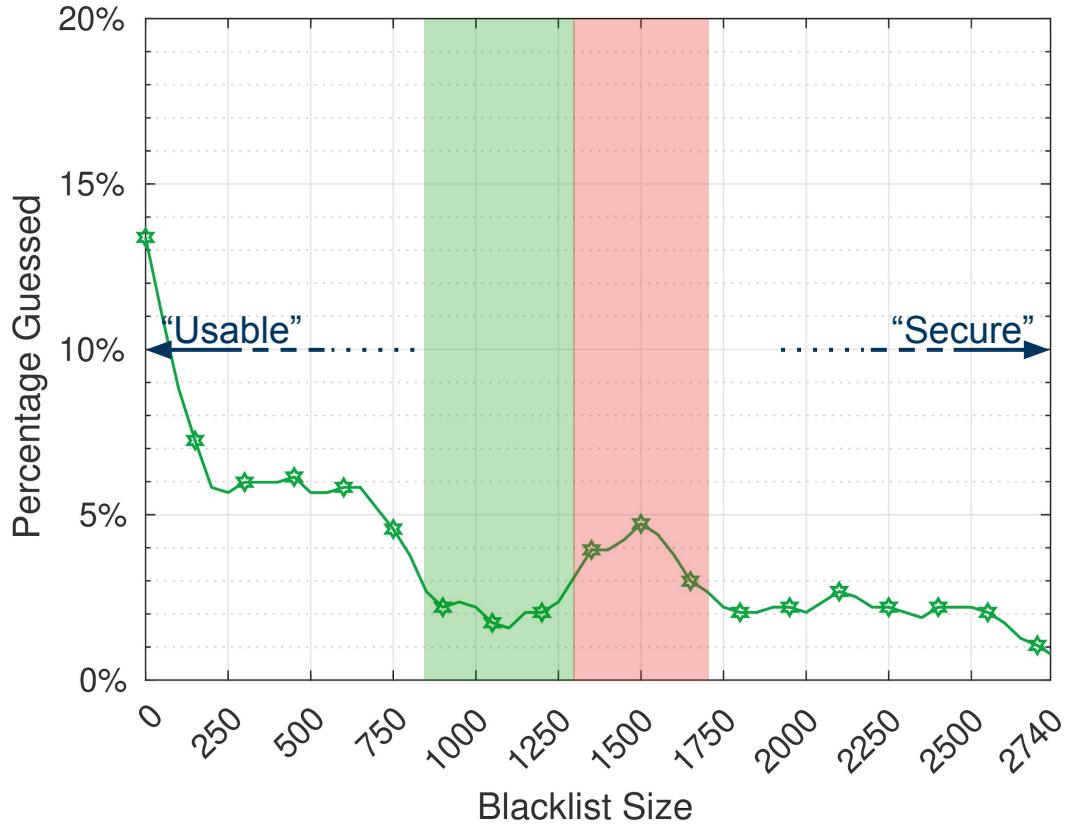


### Observations:

- iOS and Data-Driven Small offer comparable security
- Data-Driven Large drastically increases the security
- Blocklist Hitrate:



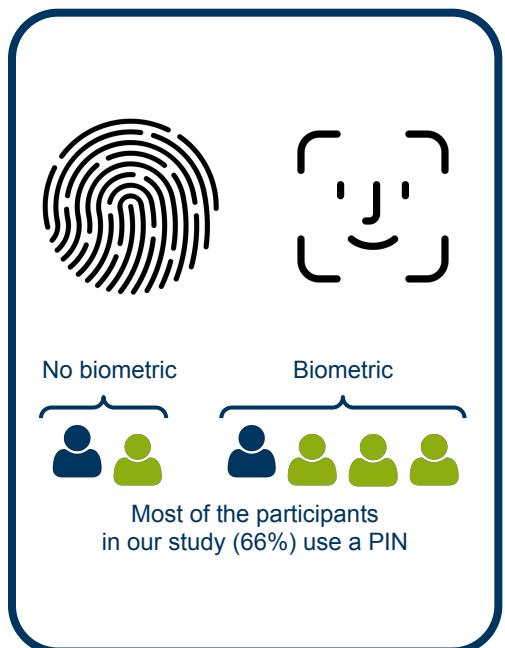
## RQ3: Balancing Security and Usability



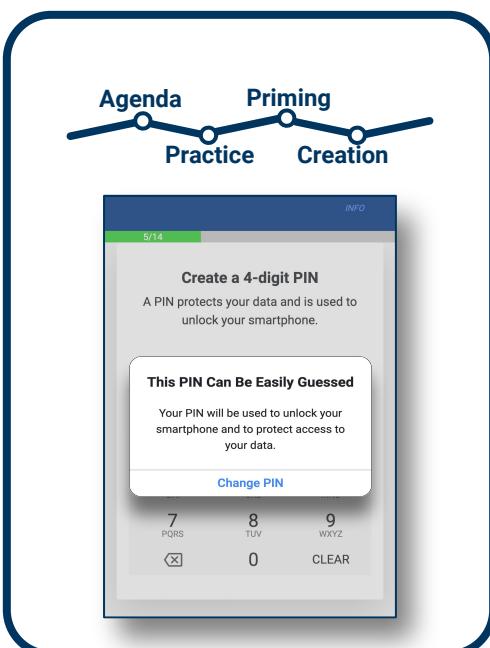
### Observations:

- Different extrema throughout the curve
- Maxima:  
users choose popular PINs
- Minima:  
users choose unpopular PINs
- Blocking ~10% is ideal

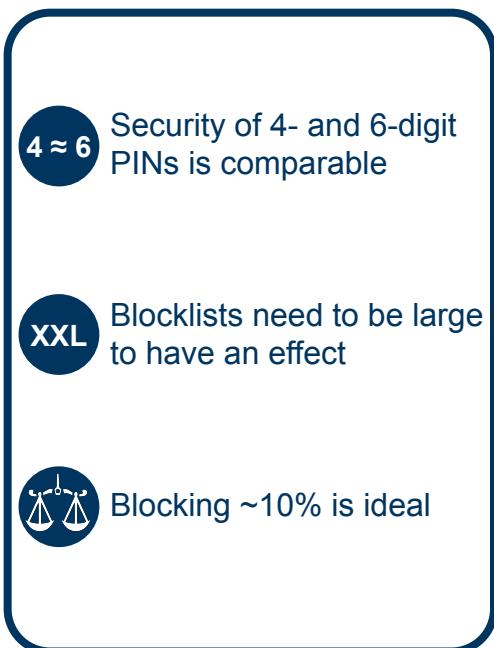
# Takeaways



## Why study PINs?



## User Study



## Results

✉ philipp.markert@rub.de

🐦 @philipp\_markert



<https://this-pin-can-be-easily-guessed.github.io>