Smartphone Users' Family, Friends, and Other Enemies

Konstantin (Kosta) Beznosov

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Laboratory for Education and Research in Secure Systems
Department of Electrical and Computer Engineering

risks to smartphones

- Malware
- Theft — on decline due to “kill switch” and activation barriers
- Loss — Find my iPhone service and alike.
- Strangers
- Social insiders
  - Coworkers
  - Spouses
  - Parents/Kids
  - Classmates/Friends
  - Etc.

scope of this talk

four studies

On the Impact of Touch ID

Cherapau, Ildar Muslukhov, Nalin
University of British Columbia,
{icherapau,ildarm,nalin,bezn

Snooping on Mobile Phones: Prevale

Diogo Marques,[1] Ildar Muslukhov,[2] Tiago Guerreiro,[1] Konst
[1] LaSIGE, Faculdade de Ciências
Universidade de Lisboa, Lisboon, Portugal
{dmarques, tjvg, lmc}@di.fc.ul.pt
[2] Department of Electrical and Computer Engineering
University of British Columbia, Vancouver, BC, Canada
{ildarm,konstantin}@ece.ubc.ca

ow Your Enemy: The Risk o

Yazan Boshmaf
The University of British Columbia
Vancouver, BC, Canada
boshmaf@ece.ubc.ca
Jonathan Lester
Minia Research Center
Palo Alto, CA, USA
jlester@gmail.com

Smartphones /

Android Users in the Wild:
Their Authentication and Usage Be

Mahfouz[a,b], Ildar Muslukhov[a], Konst
Electrical and Computer Engineering
332 Main Mall, Vancouver,
Department, Minia Uni

an be confi-
obile OS

smartphone study

- semi-structured interviews (N=22) — Nov. 2011
  - users' concerns with sensitive data.
- MTurk survey (N=724) — early 2012
  - strangers vs. insiders

I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "**Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders**," In Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (Mobile HCI), August 27 - 30, 2013, Munich, Germany, pp. 271-280.

Android study

- Android monitoring app (N=41)
- 20 days between 12/20/2014 and 3/13/2015
- (un)locking and app usage behaviour

A. Mahfouz, I. Muslukhov, K. Beznosov "**Android Users in the Wild: Their Authentication and Usage Behaviour**" in *Pervasive and Mobile Computing*, Elsevier, 2016.

Touch ID study

small-scale (N=90)

- **in-person survey**
- late 2014
- iPhone model and passcode length verification

online larger-scale (N=374)

- **MTurk survey (US/95%)**
- early 2015
- unlocking method and iPhone model verification

I. Cherapau, I. Muslukhov, N. Asanka, and K. Beznosov, "**On the Impact of Touch ID on iPhone Passcodes**," in Proceedings of Symposium On Usable Privacy and Security (SOUPS), Ottawa, Canada, July 22-24, 2015, pp. 257—276.

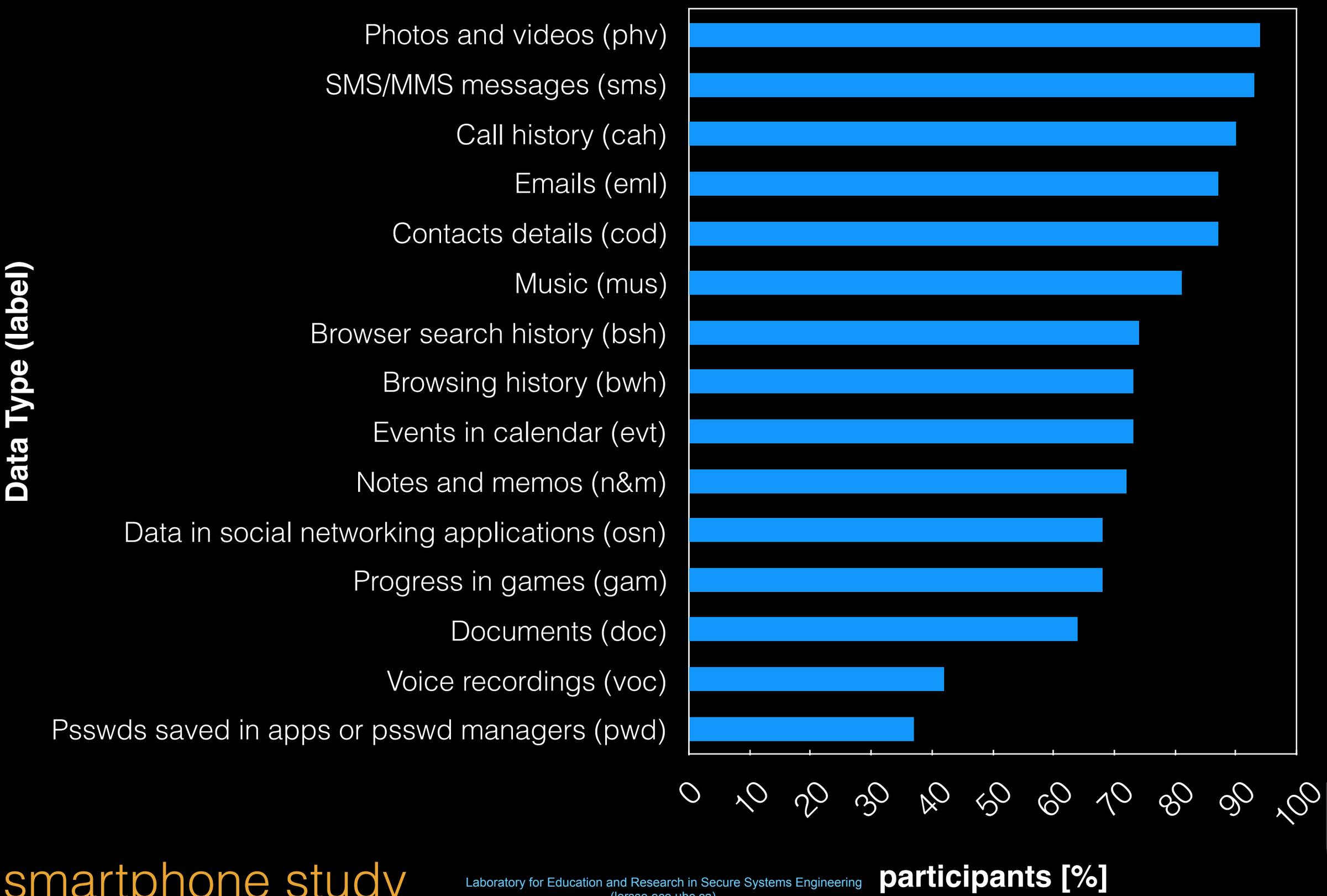
snooping study

- privacy-preserving MTurk survey (N=1,381) — 2015
- MTurk followup (N=653) — early 2016

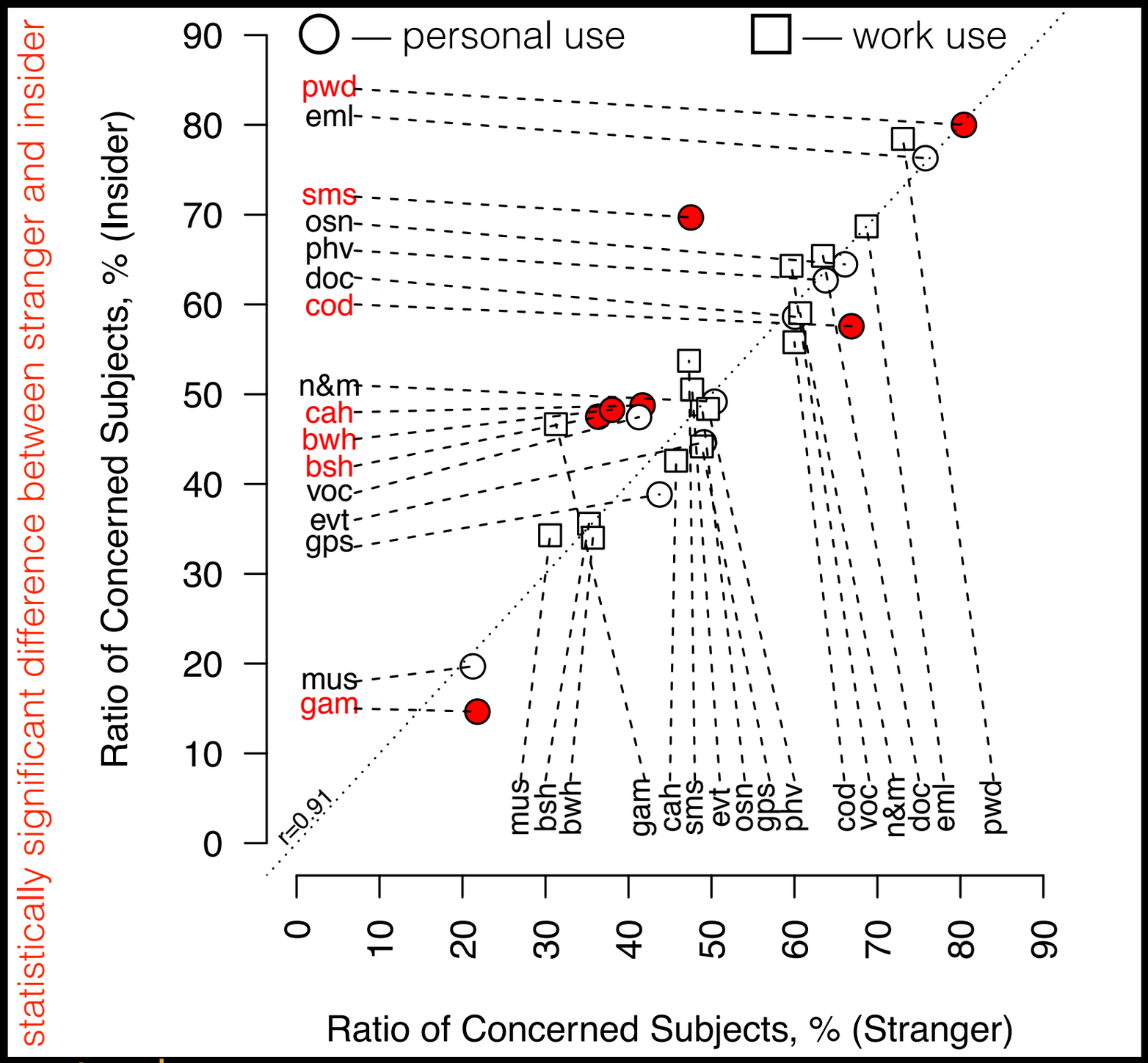
D. Marques, I. Muslukhov, T. Guerreiro, L. Carriço, K. Beznosov, "**Snooping on Mobile Phones: Prevalence and Trends**" in Proceedings of Symposium On Usable Privacy and Security (SOUPS), Denver, CO, USA, June 22-24, 2016, pp. 159–174.

findings

smartphones contain various data



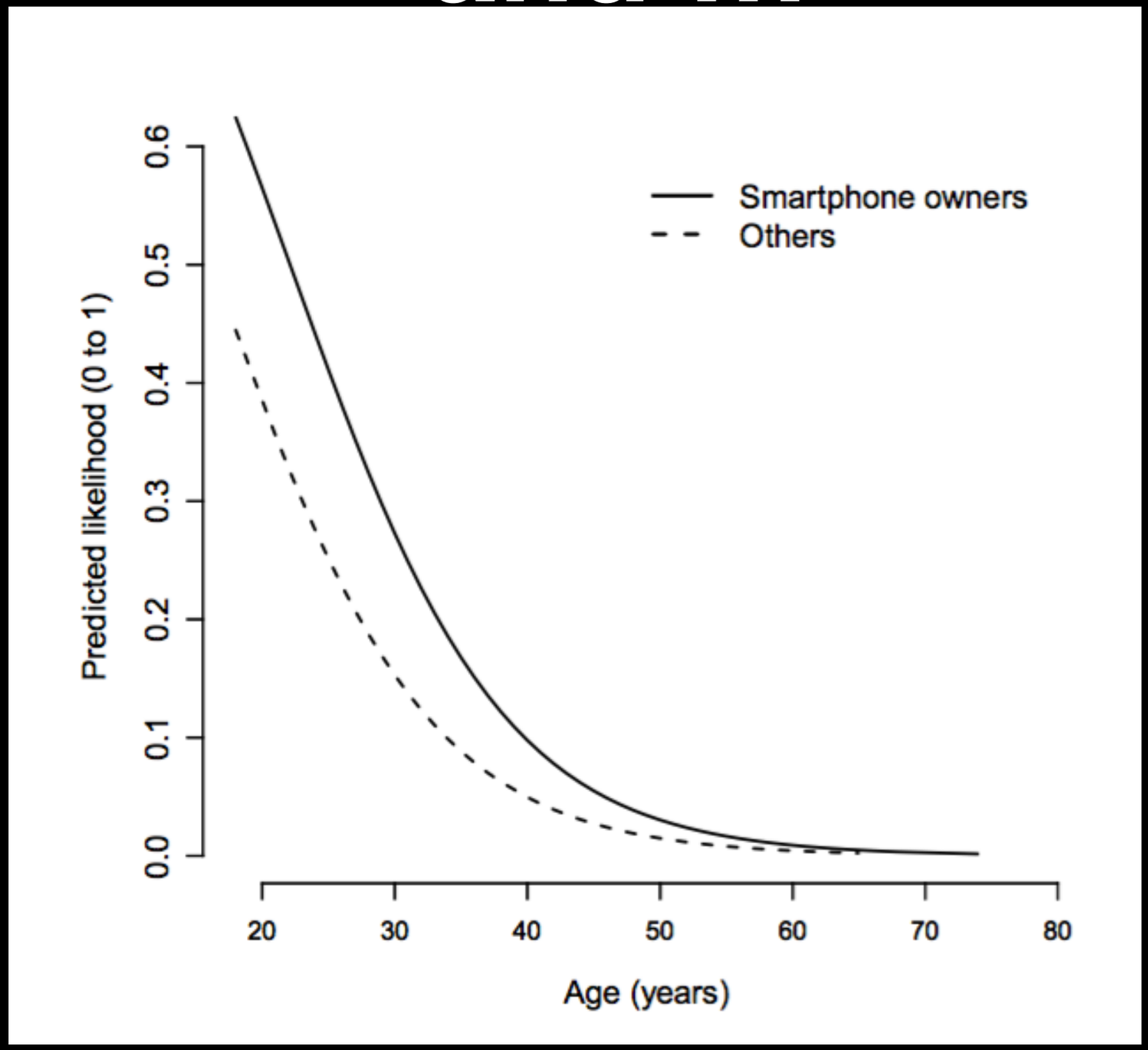
users' concerns about insiders and strangers are comparable



smartphone study

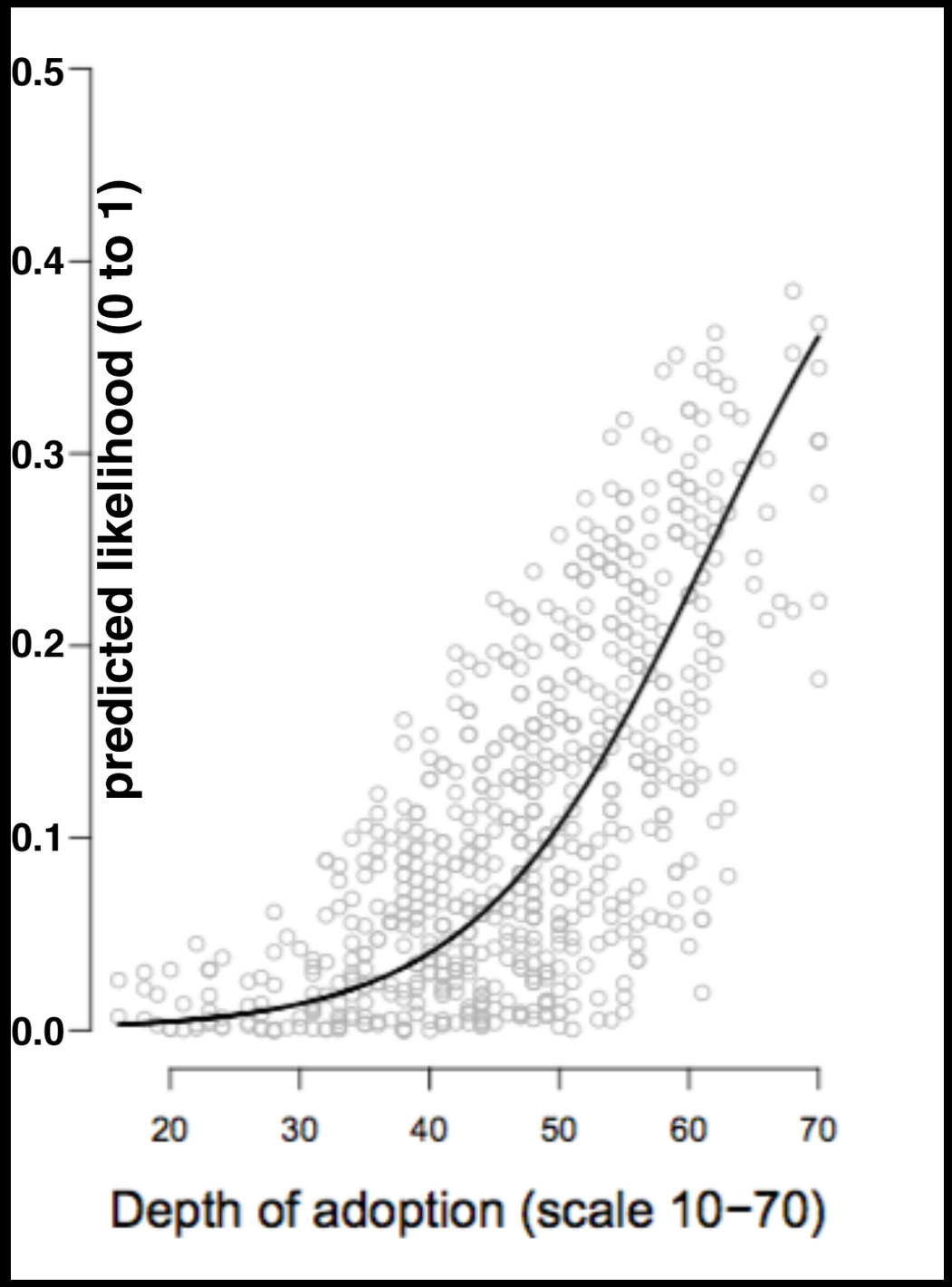
20% of US adults had engaged in snooping in a 1-year period

likelihood correlates with age and …



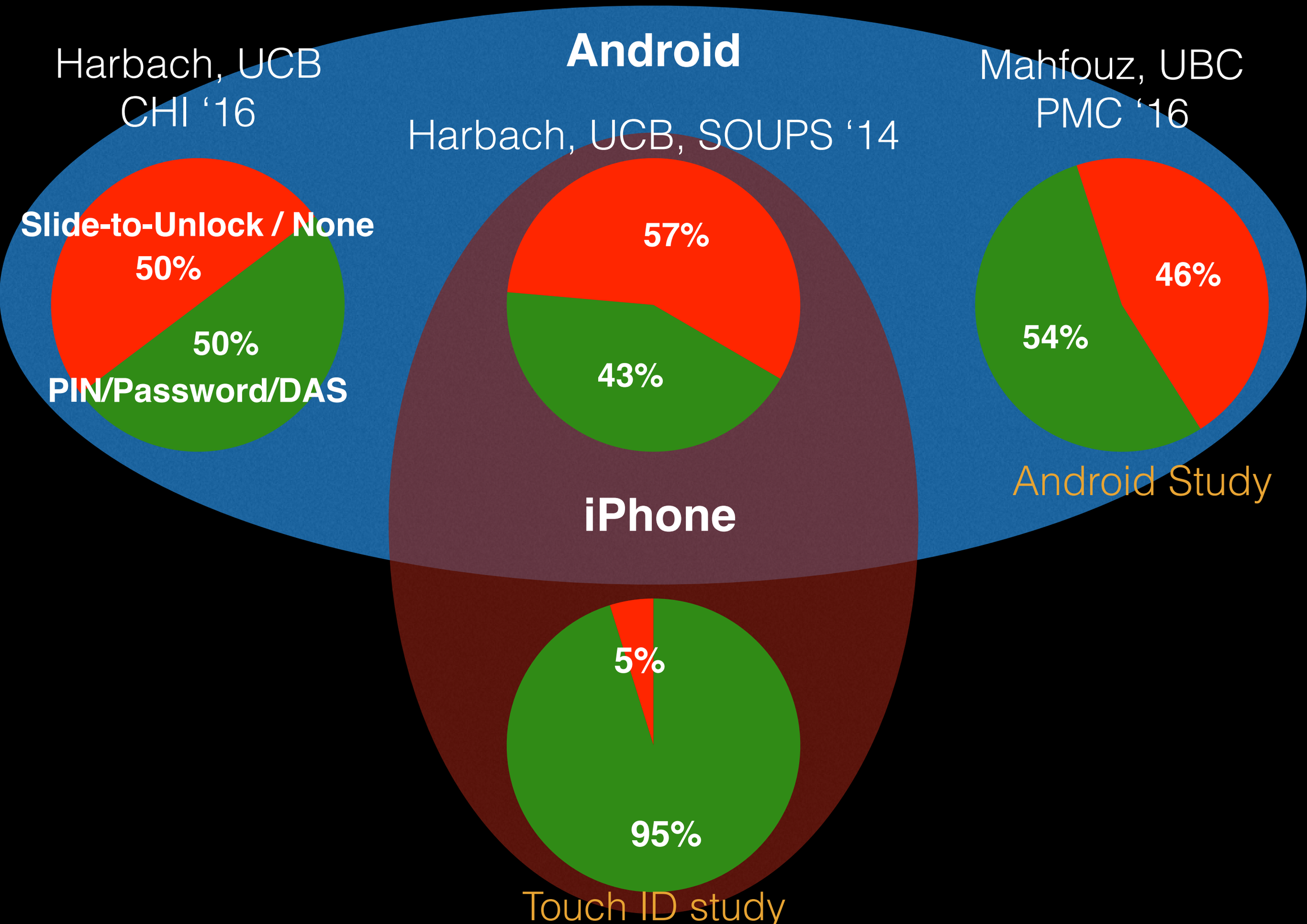
snooping study

… and with depth of adoption

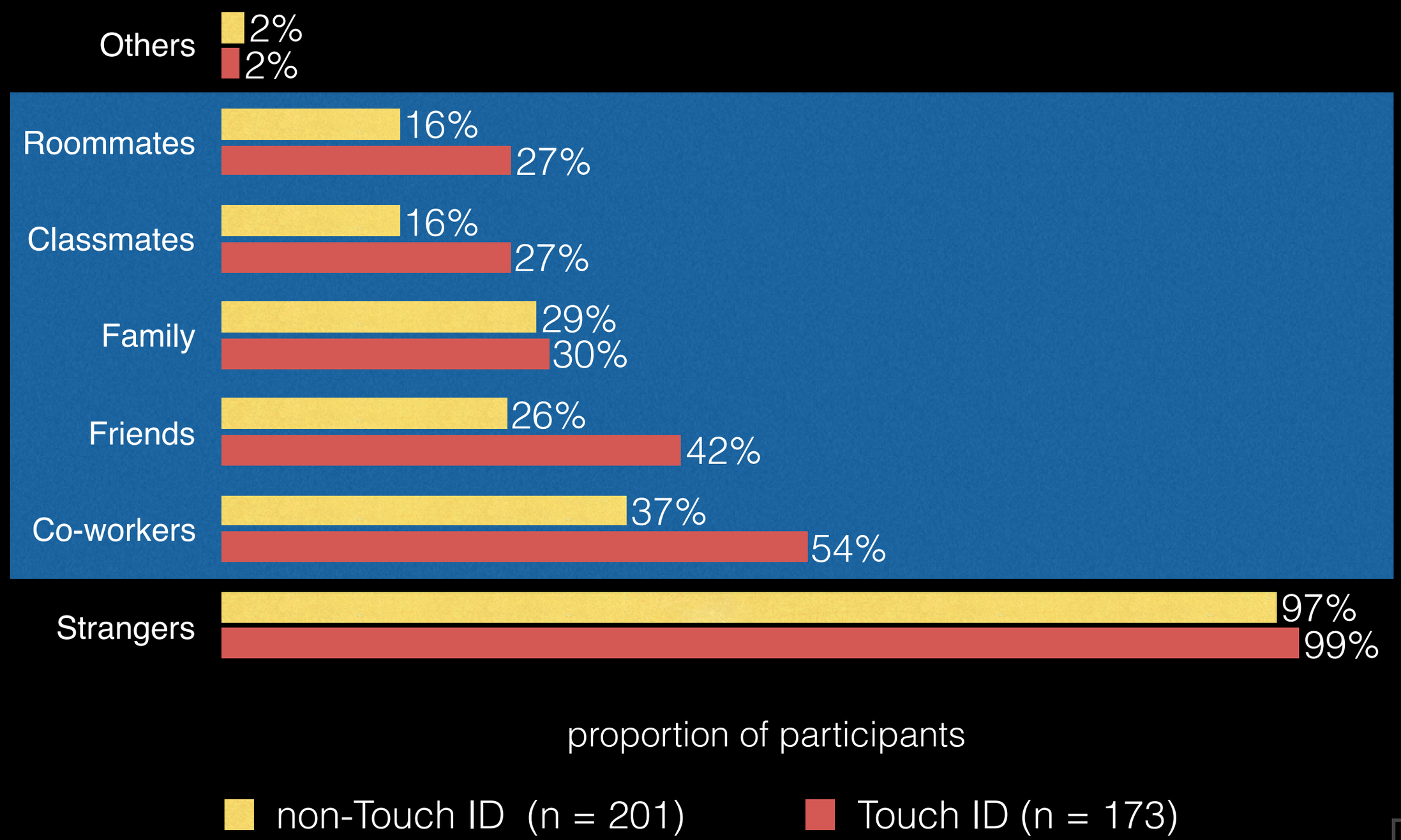


snooping study

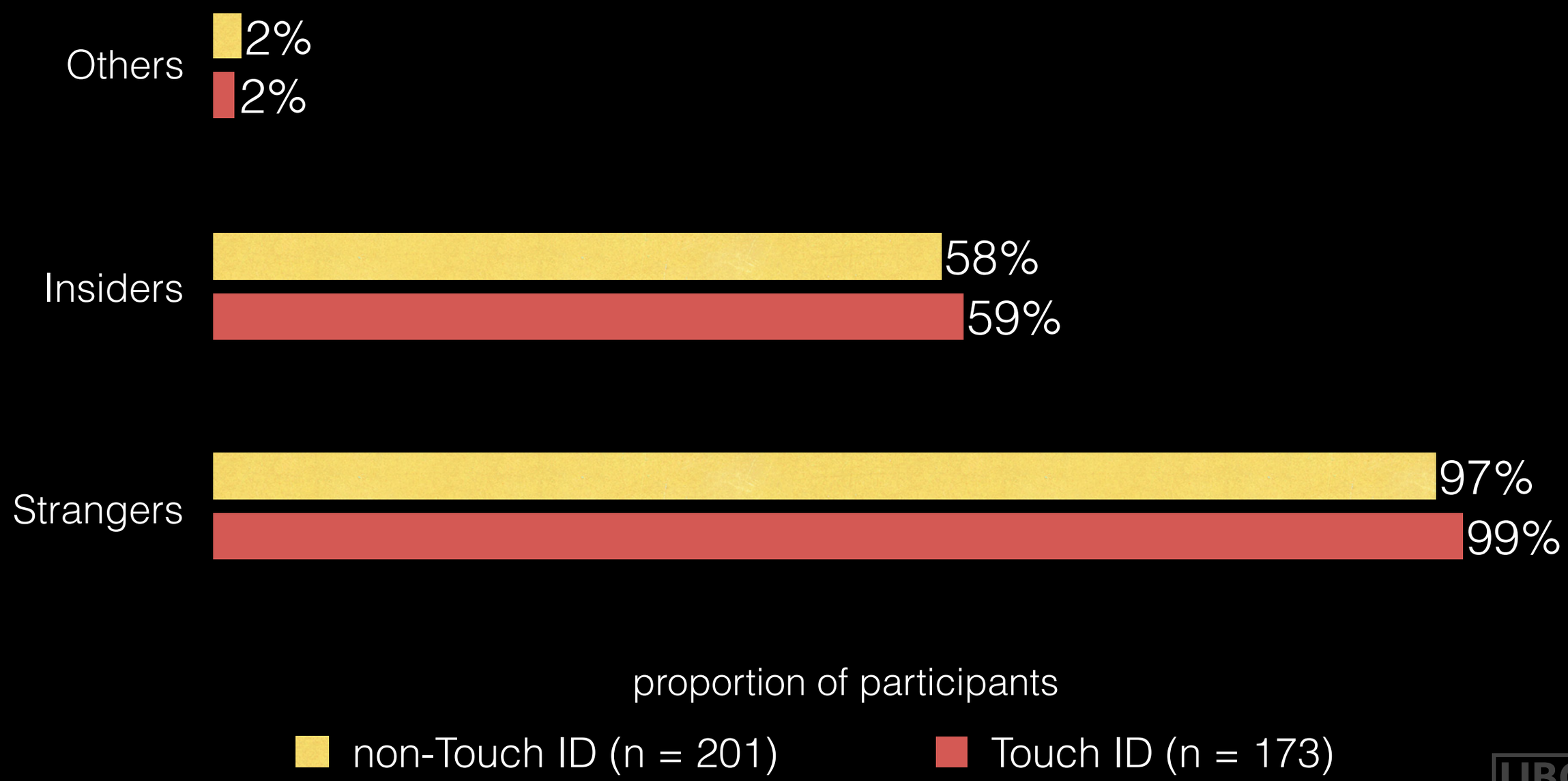
adoption of locking



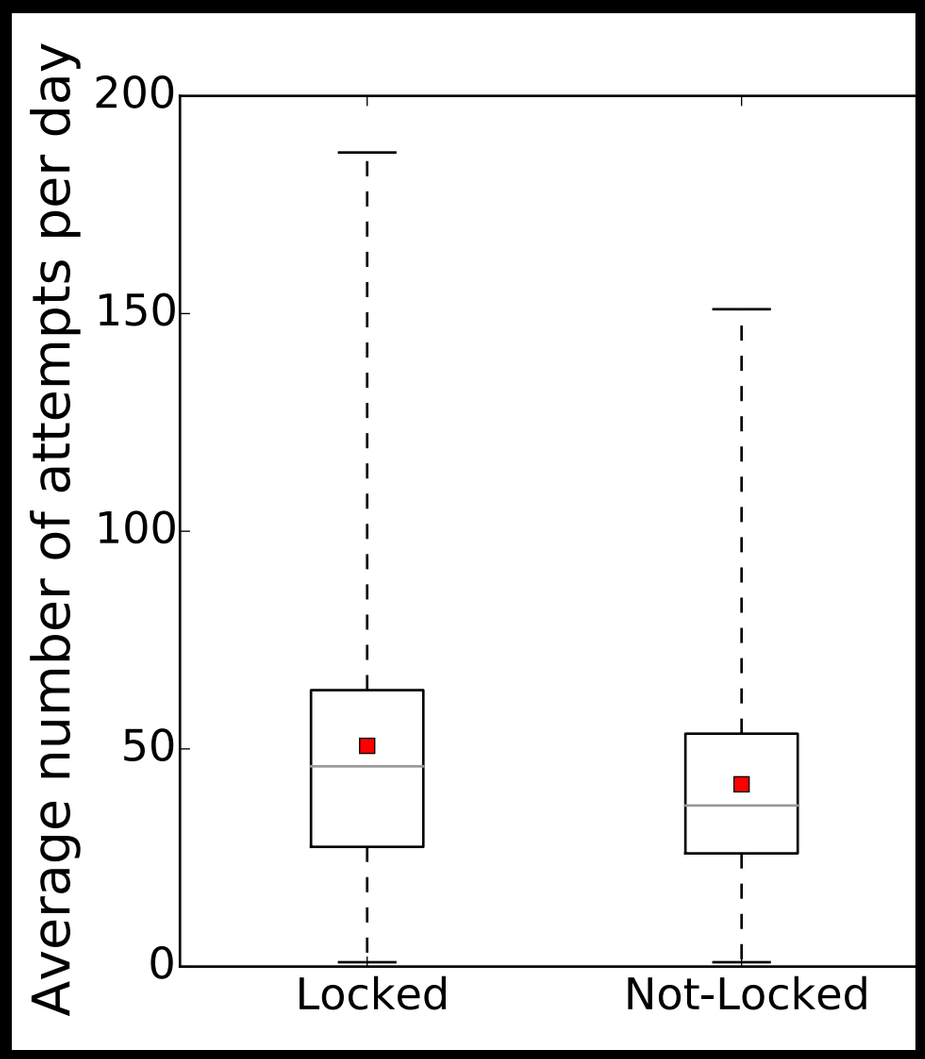
users lock their phones against



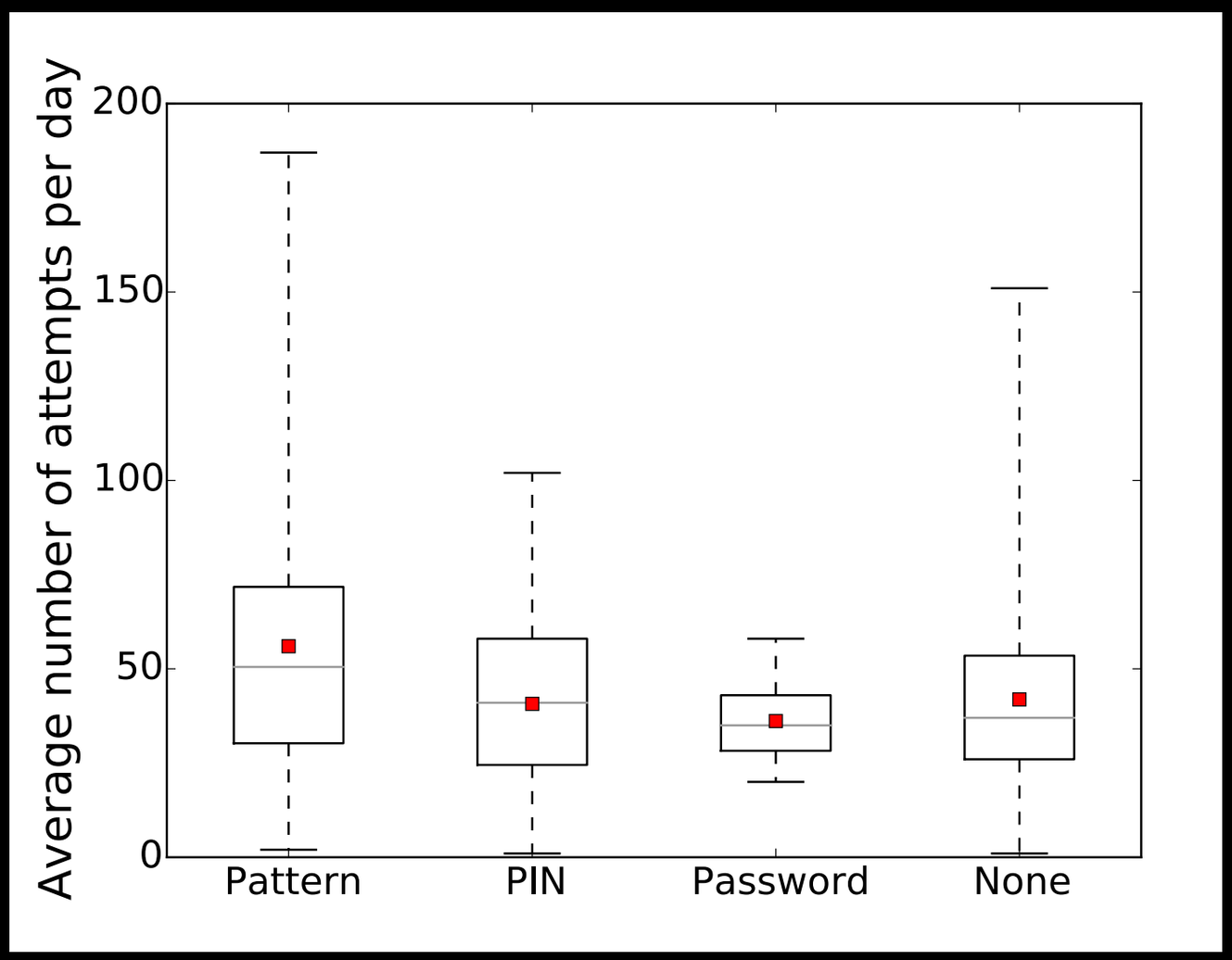
users lock their phones against



those who lock, use more often …



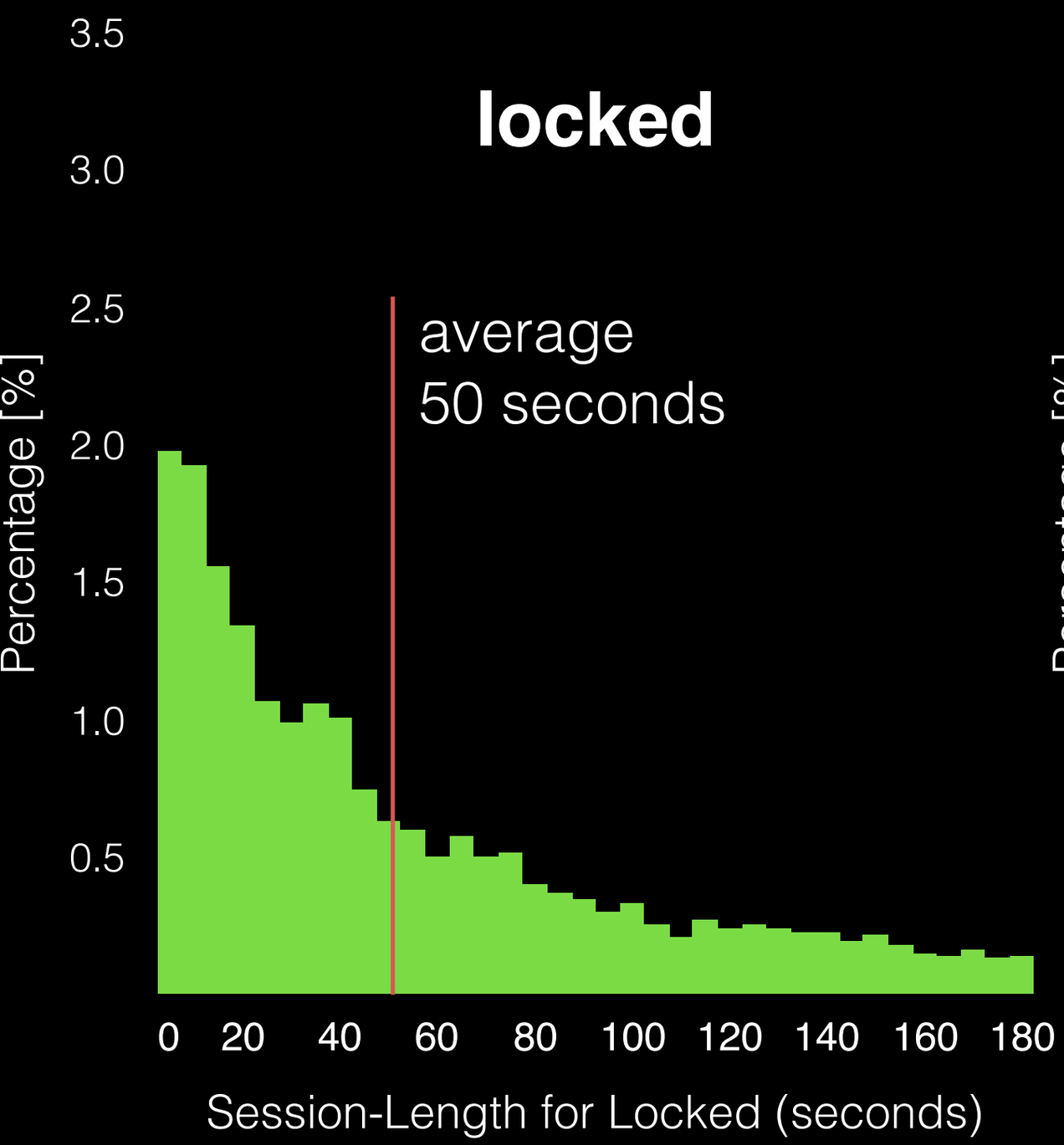
51 41

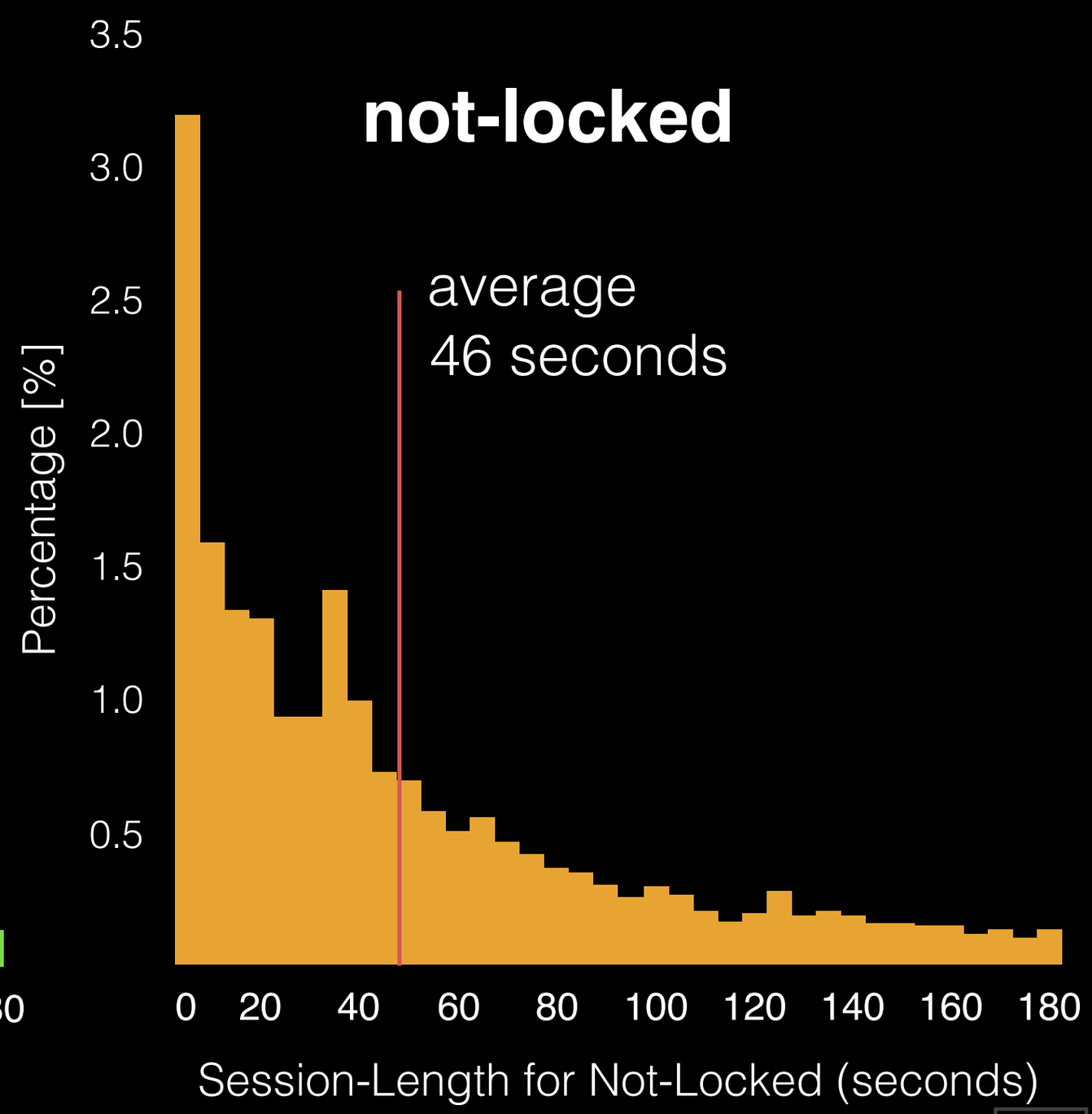


56 42 36 41

Android study (N=41)

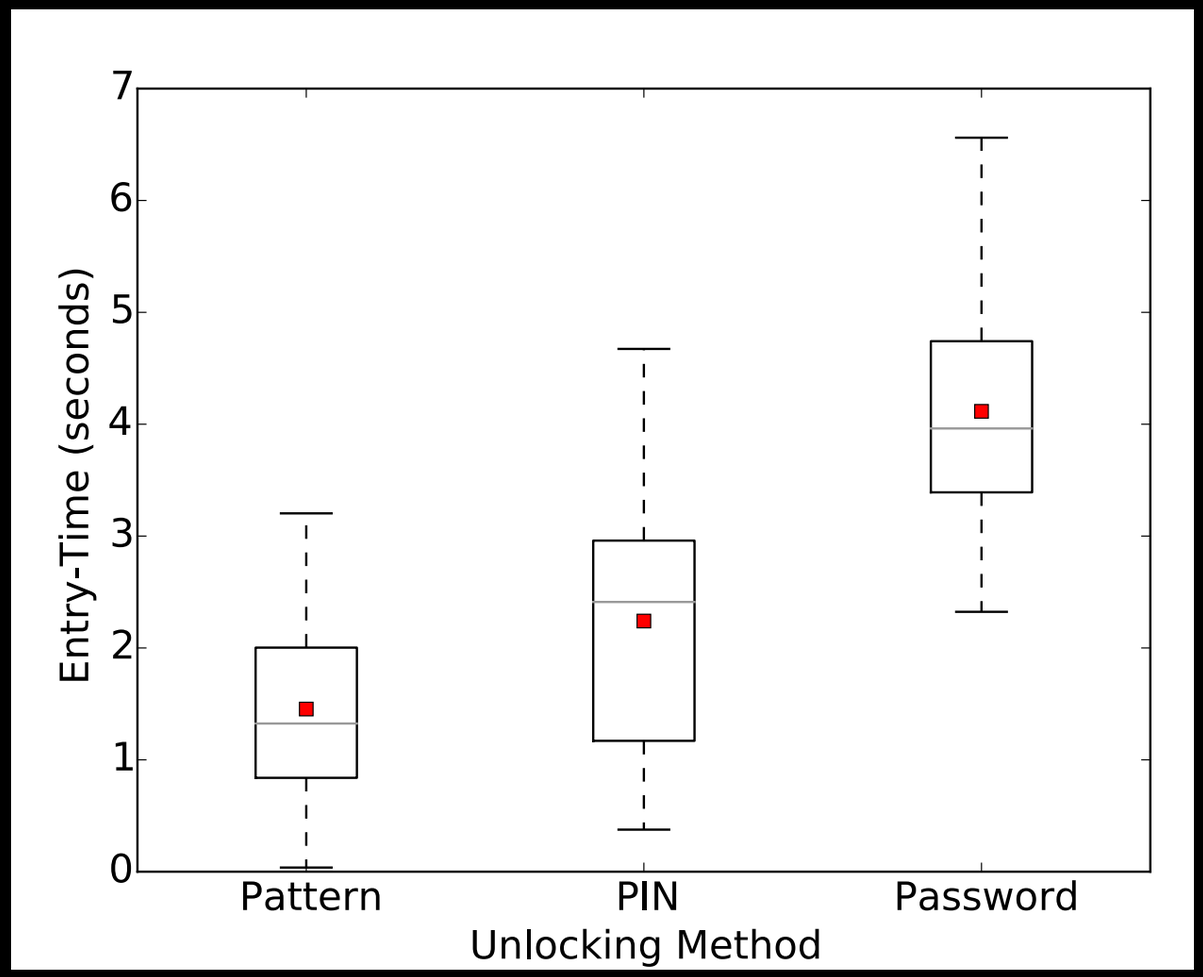
… and for longer, each time



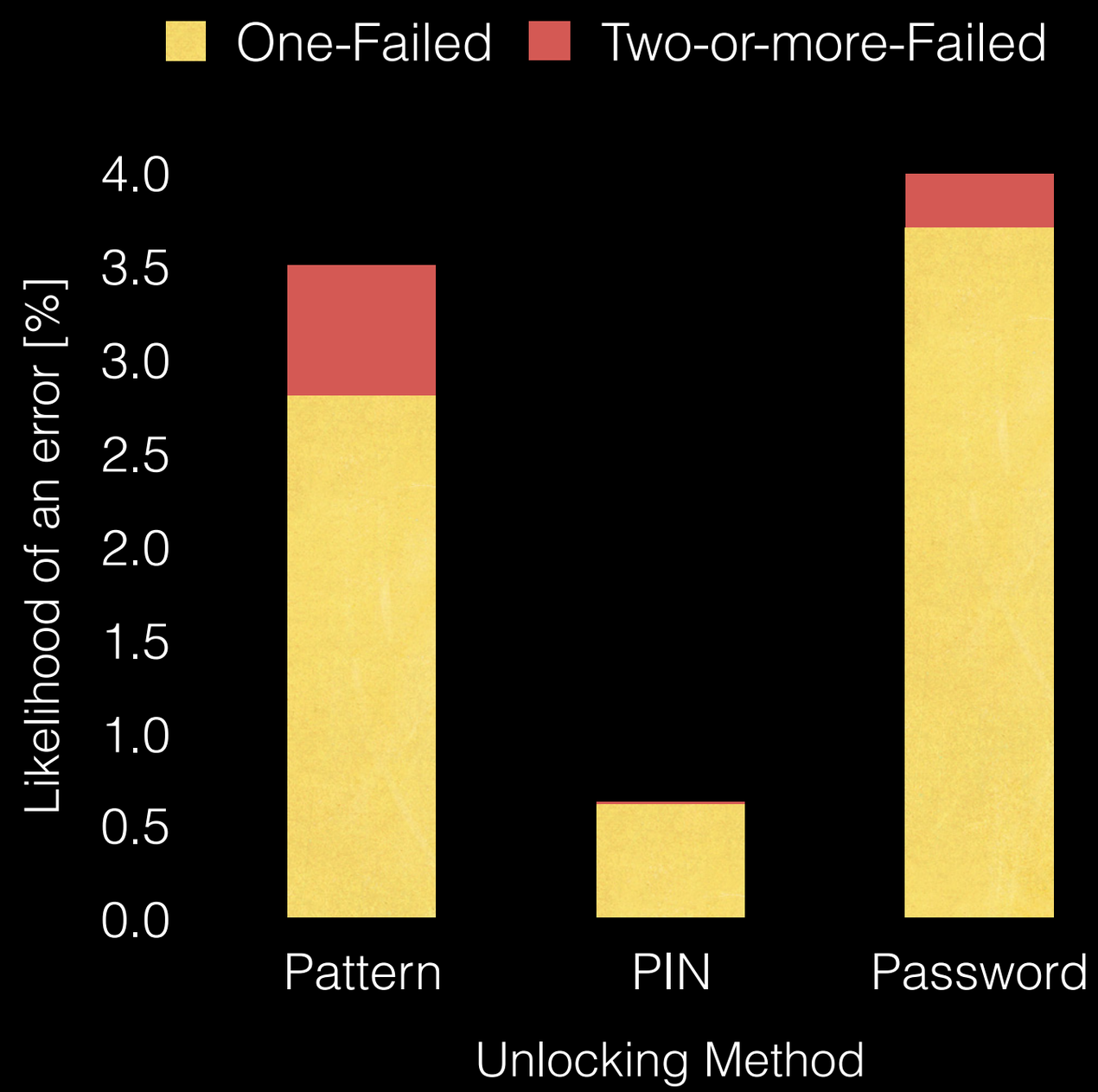


Android study (N=41)

unlocking methods vary in cost

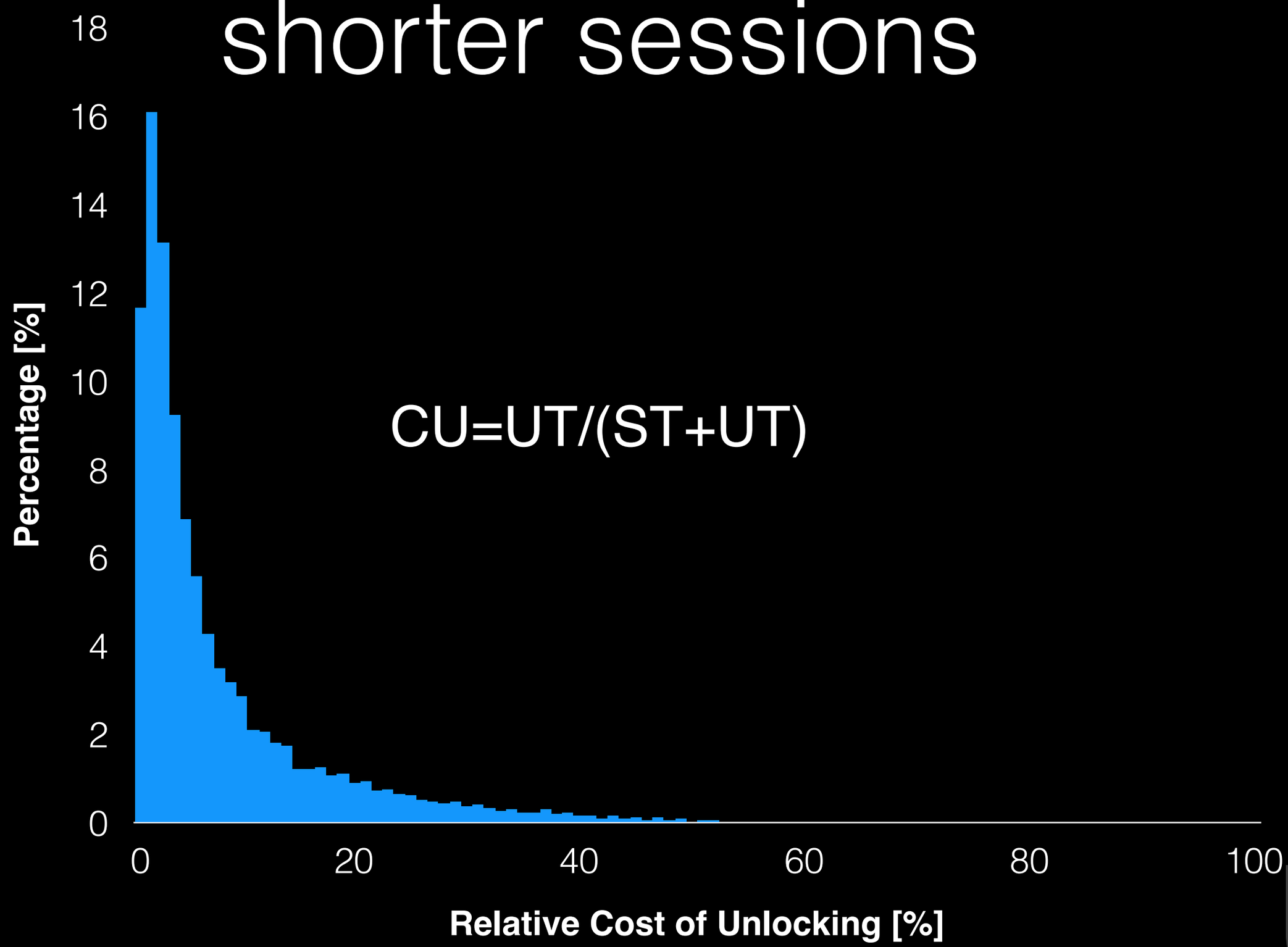


1.7 2.5 4.1



Android study (N=22)

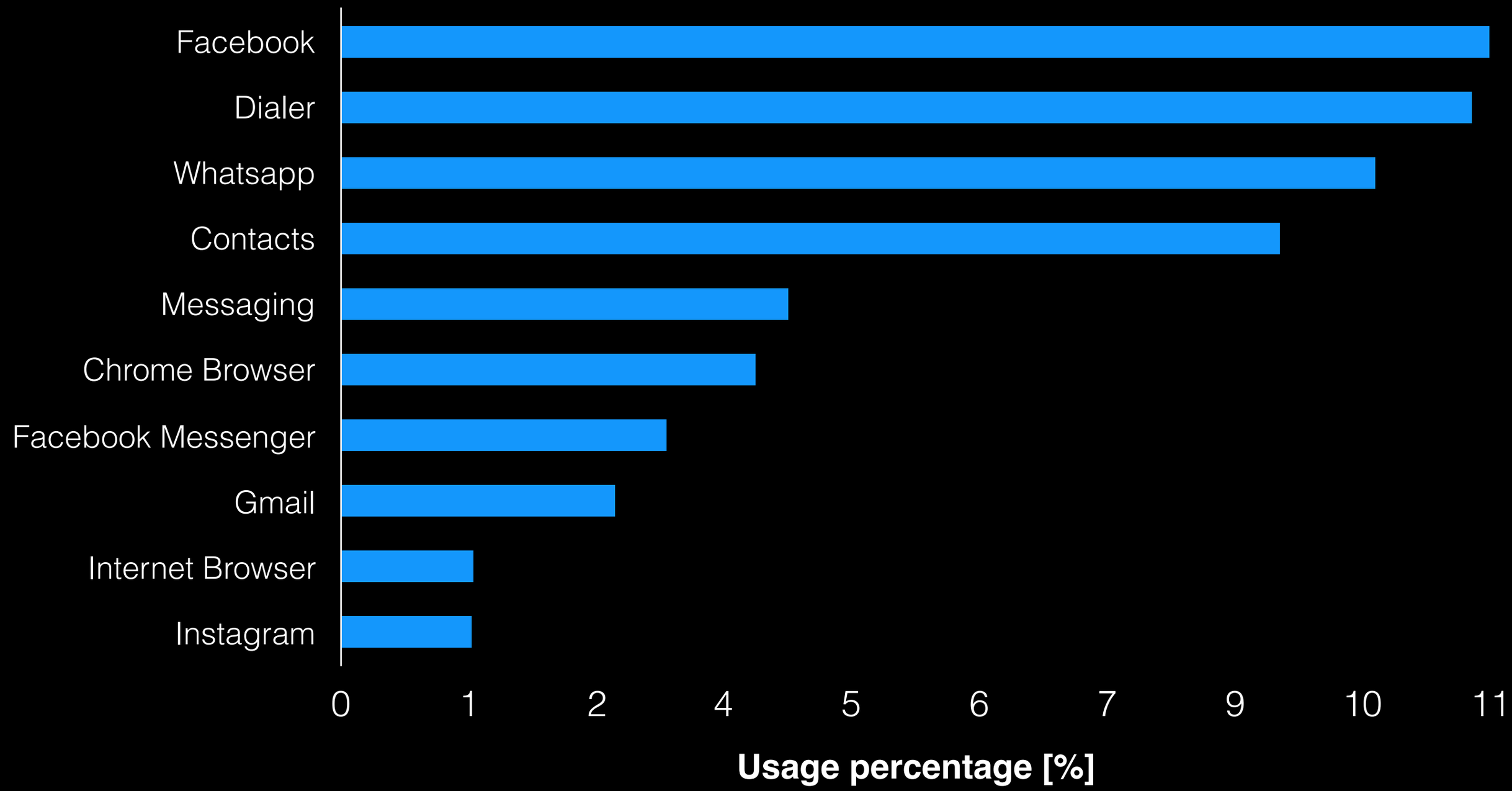
30-80% cost for shorter sessions



CU=UT/(ST+UT)

Android study (N=41)

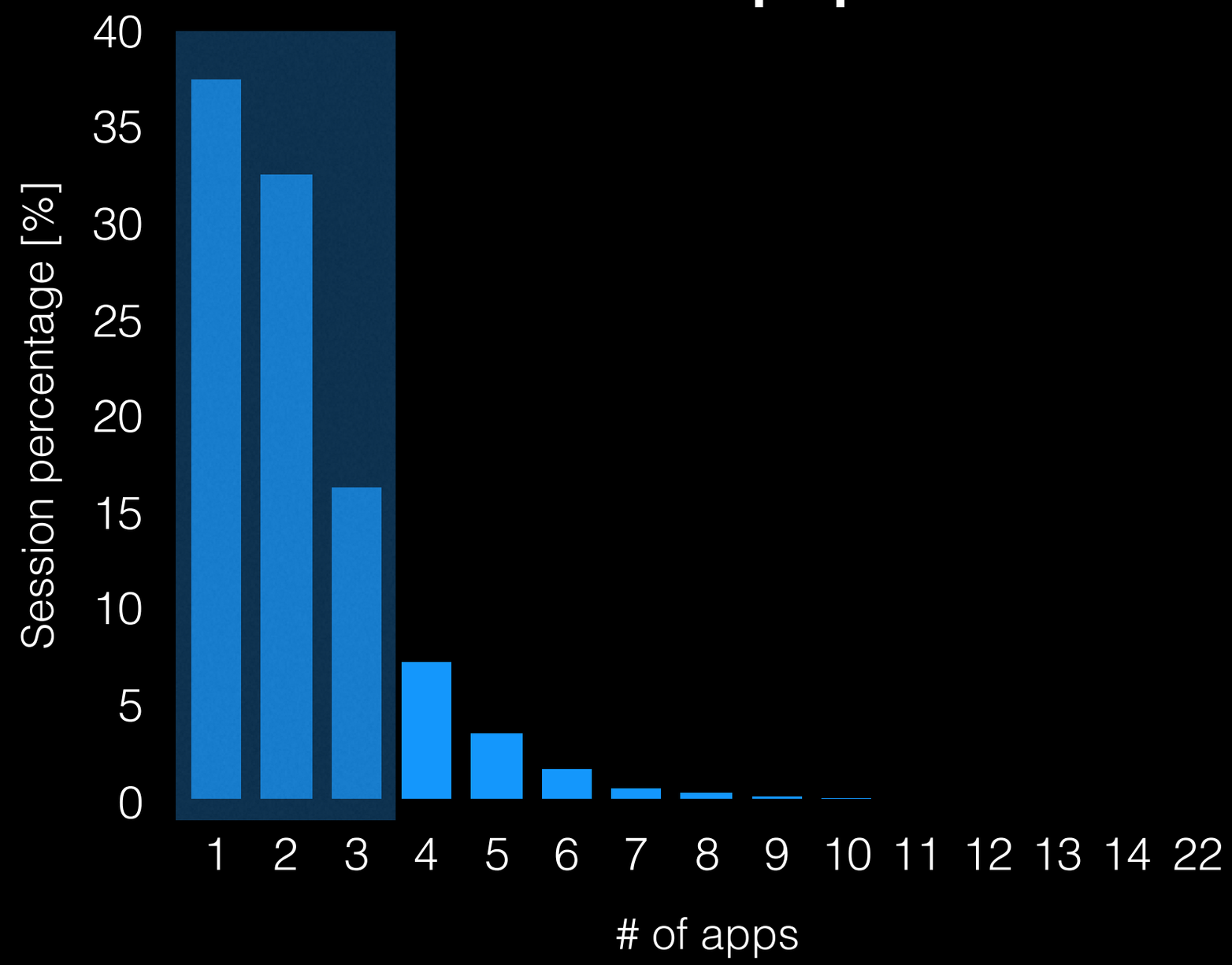
top ten applications comprise 57% of all observed sessions



564 apps observed in the study

Android study (N=41)

85% of sessions involved 1-3 apps



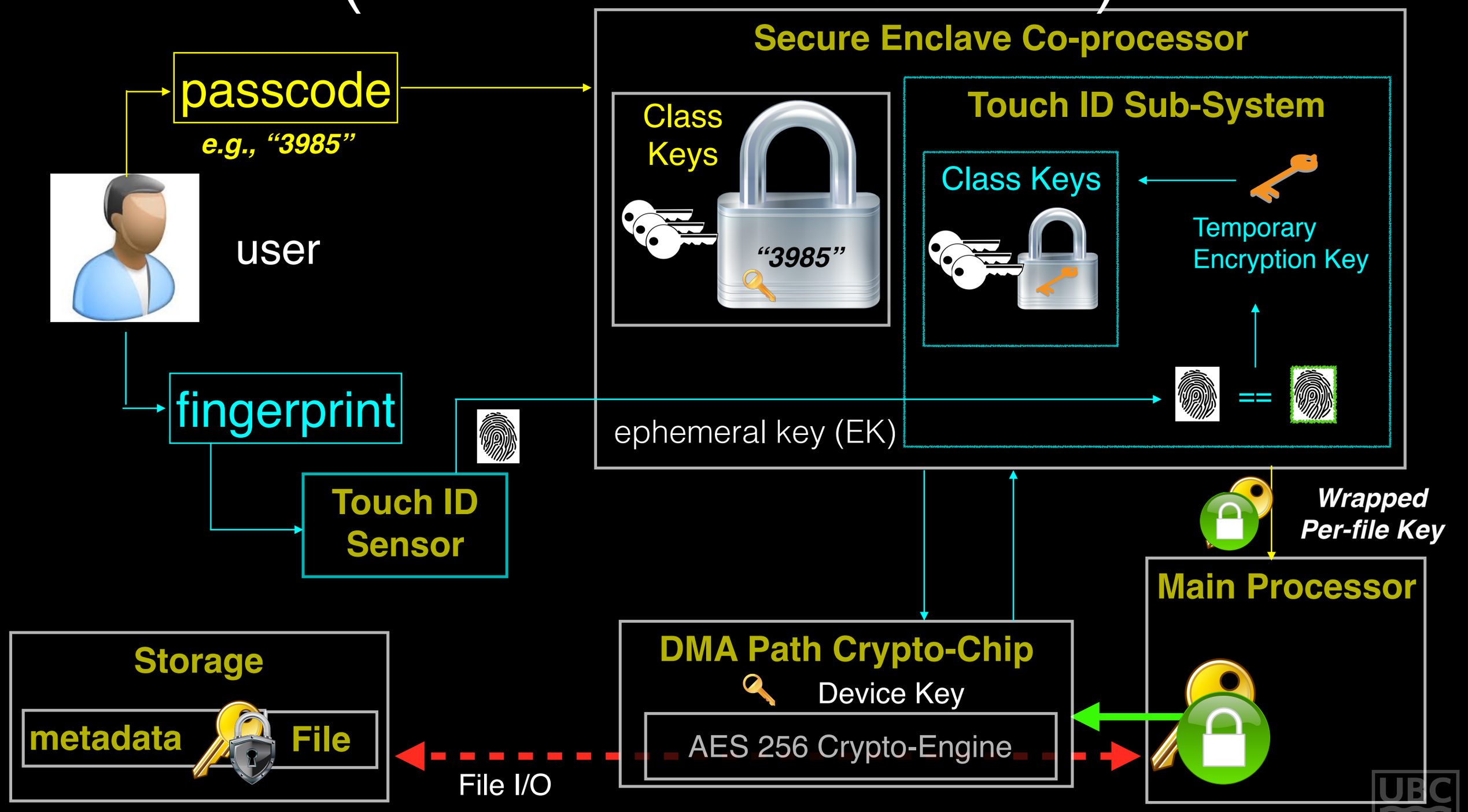
25 seconds average time for 1-2 app sessions

Android study (N=41)

Touch ID & iPhone security

how unlock works

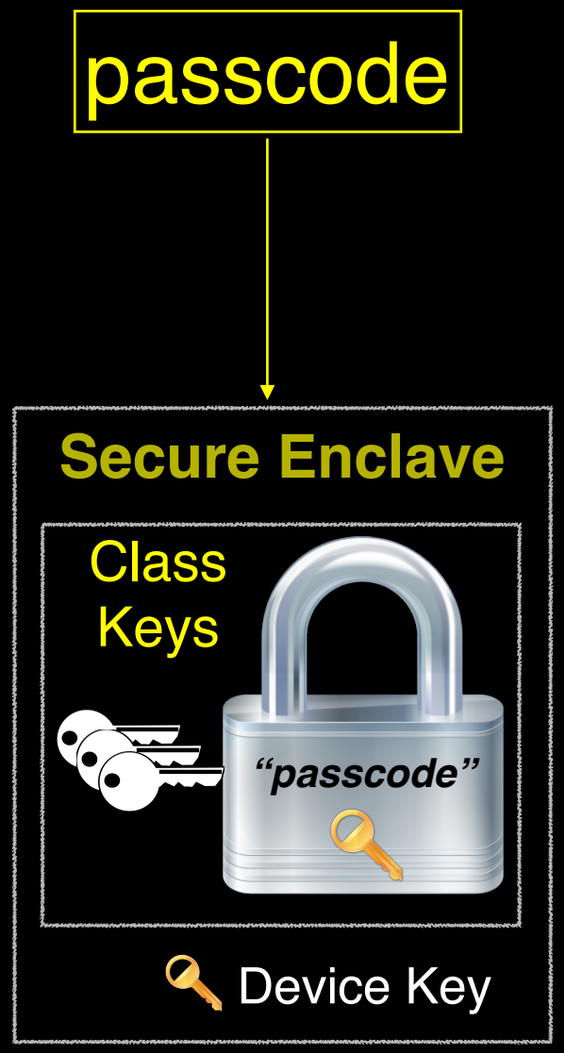
(iPhone 5s and later)



why passcode strength matters

on-device guessing attack

- 80 ms/guess
  - 6 alphanumeric — 5.5 years
  - 6 numeric — 22 hours
  - 4 numeric — 14 minutes
- requires exploitable bug in the boot-chain
  - LimeRa1n for iPhone 3GS, 4
  - Blackra1n, October 2009
  - Limera1n/greenpois0n, October 2010
  - exploit by iH8sn0w, February 2014



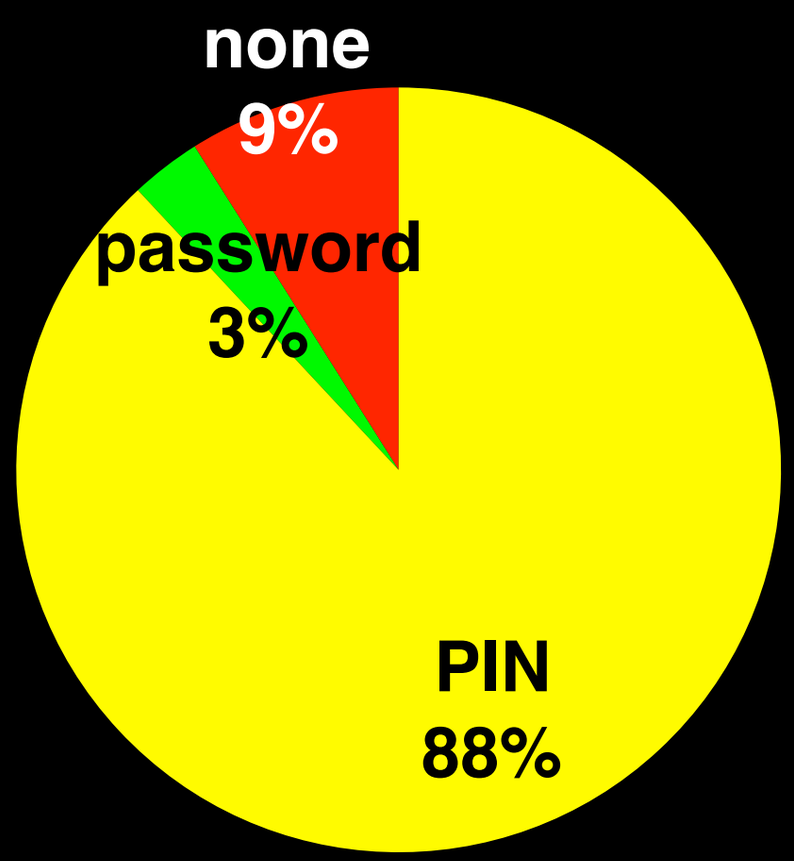
what Apple says about Touch ID

- "**Touch ID makes using a longer, more complex passcodes far more practical because users won't have to enter it as frequently**".

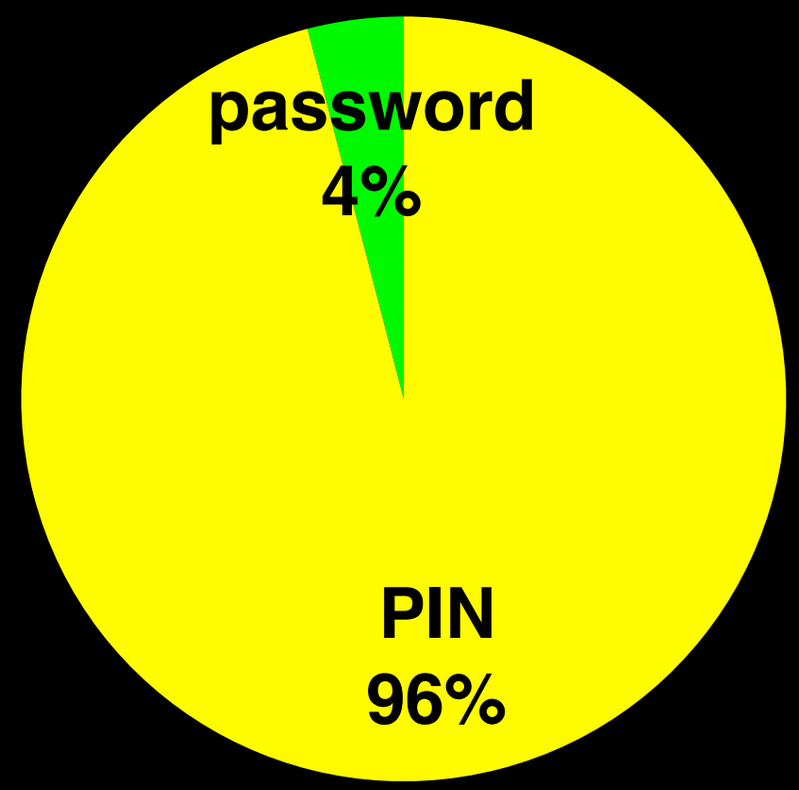
- "The stronger the user passcode is, the stronger the encryption key becomes. Touch ID can be used to enhance this equation by **enabling the user to establish a much stronger passcode than would otherwise be practical**. This increases the effective amount of entropy protecting the encryption keys used for Data Protection without adversely affecting the user experience of unlocking an iOS device multiple times throughout the day".

Touch ID has had no significant impact on iPhone passcodes

H_2^{null} *— Availability of Touch ID has no effect on* ***ratio of users who lock their iPhones****.*



MTurk

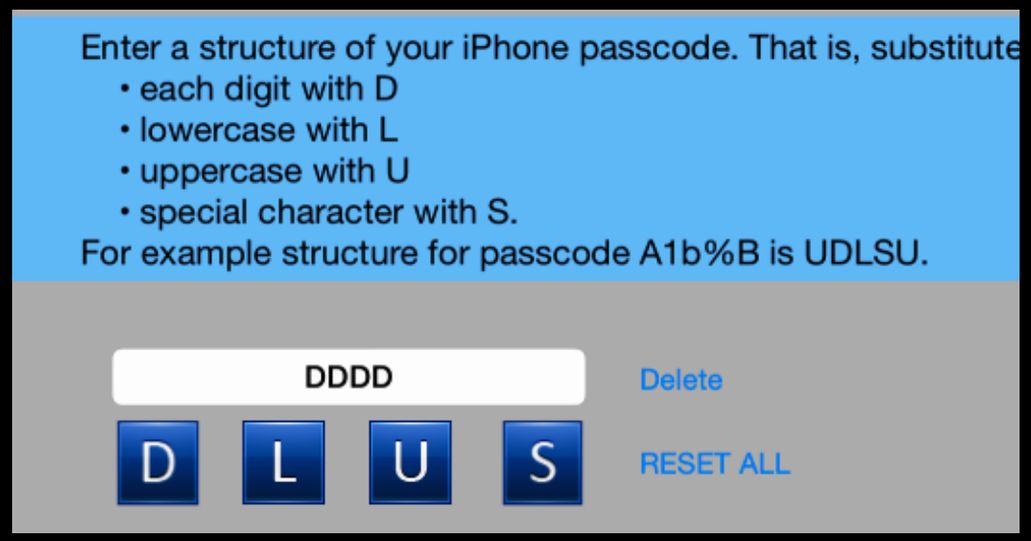


non-Touch ID users (n=201)

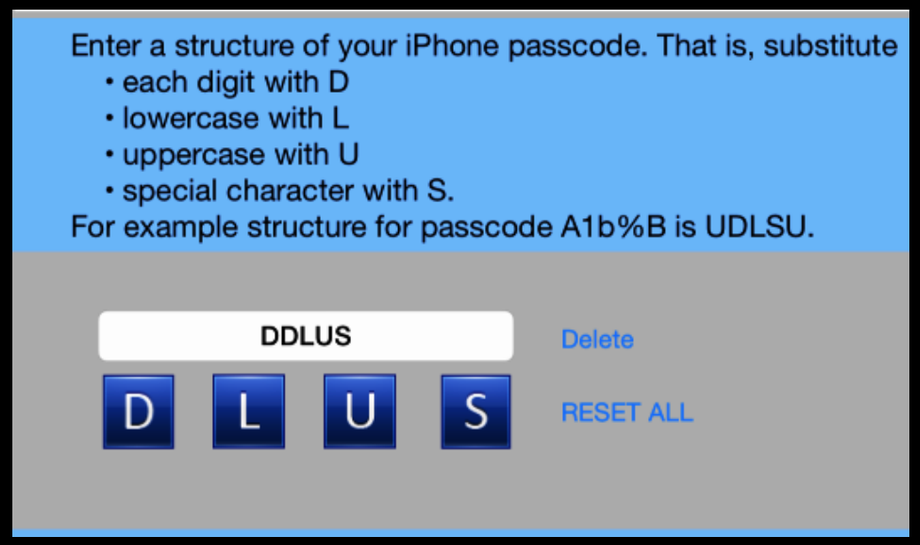
Touch ID users (n=173)

H_1^{null} *— Use of Touch ID has no effect on* ***the entropy of passcodes*** *used for iPhone locking.*

passcode info collected



PIN

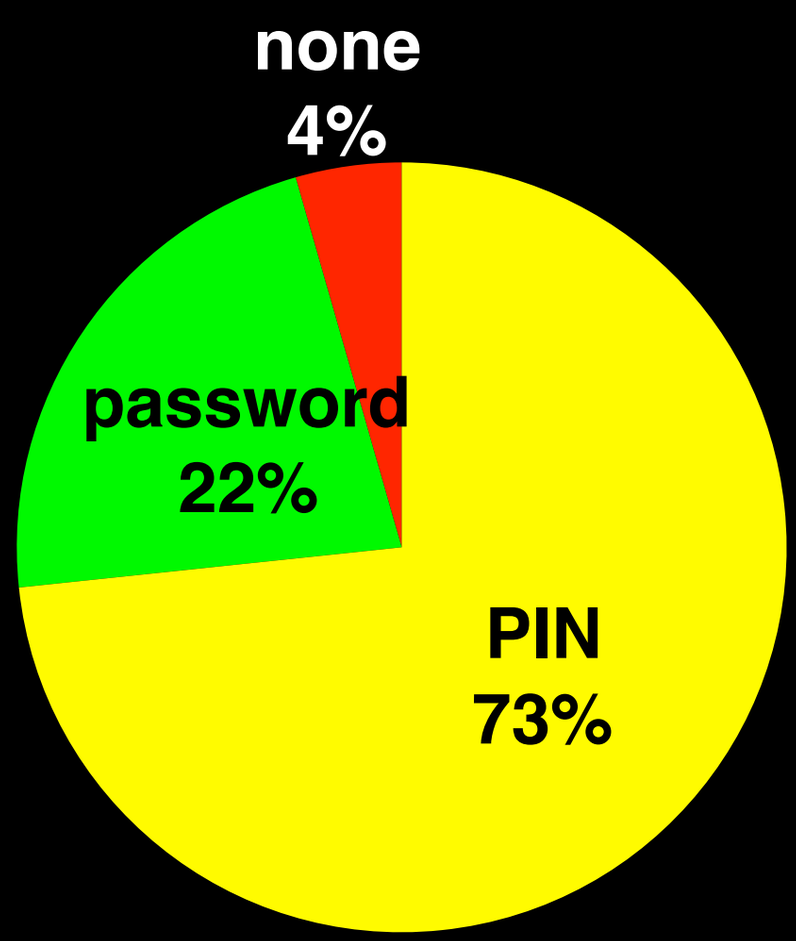


password

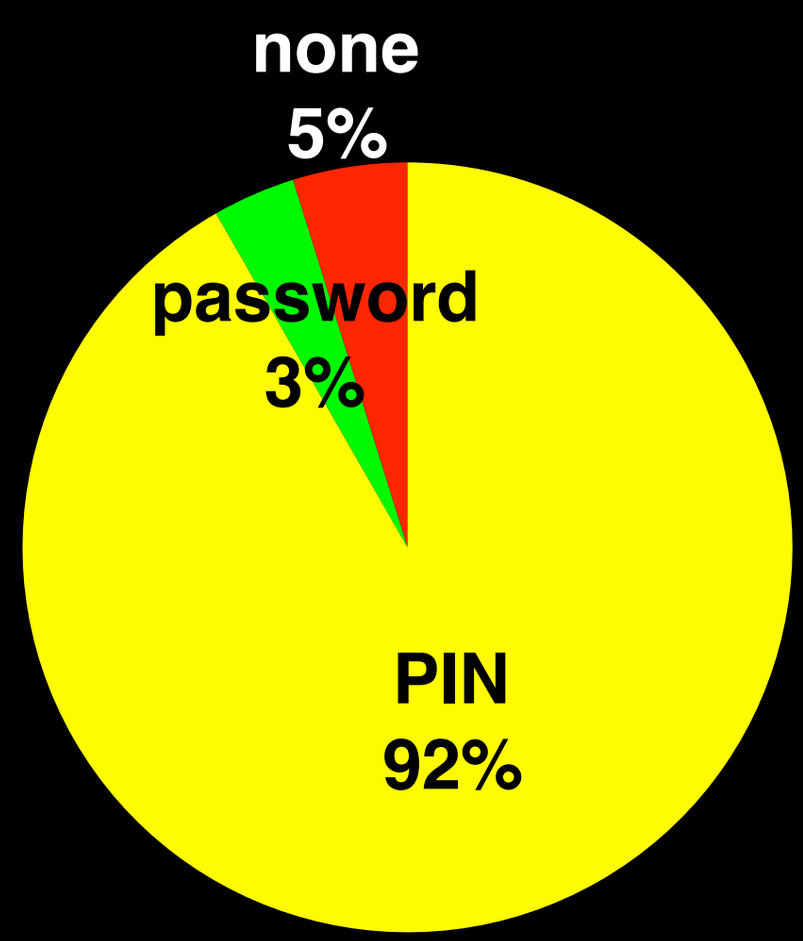
passcodes are weak

	in-person (n=90)		MTurk (n=374)	
	zero-order entropy	time to crack	zero-order entropy	time to crack
non-Touch ID	**15.6**	1h10m	**14.1**	30 minutes
Touch ID	**15.9**	1h20m	**16.5**	2 hours

most use 4-digit PINs

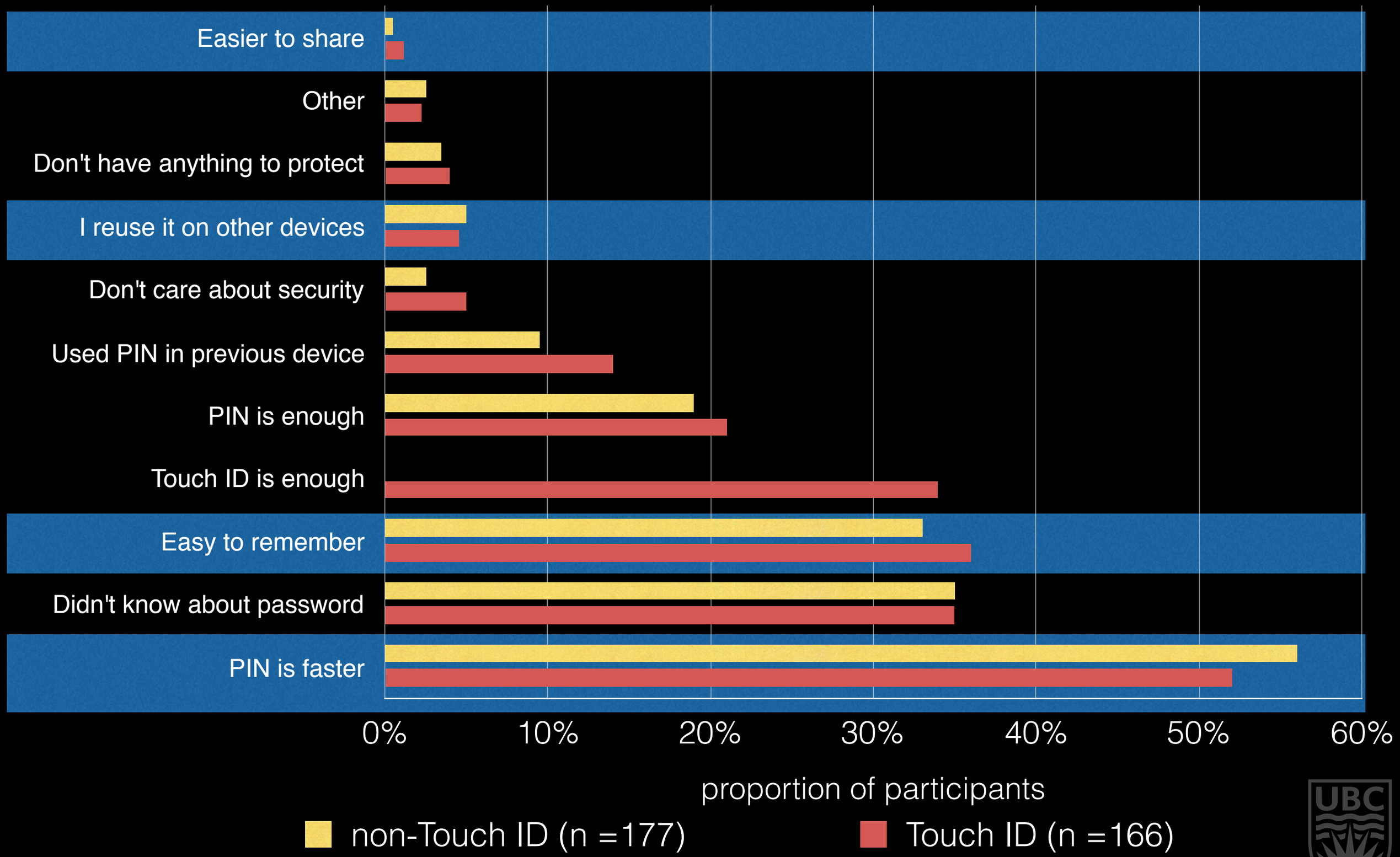


in-person (n=90)



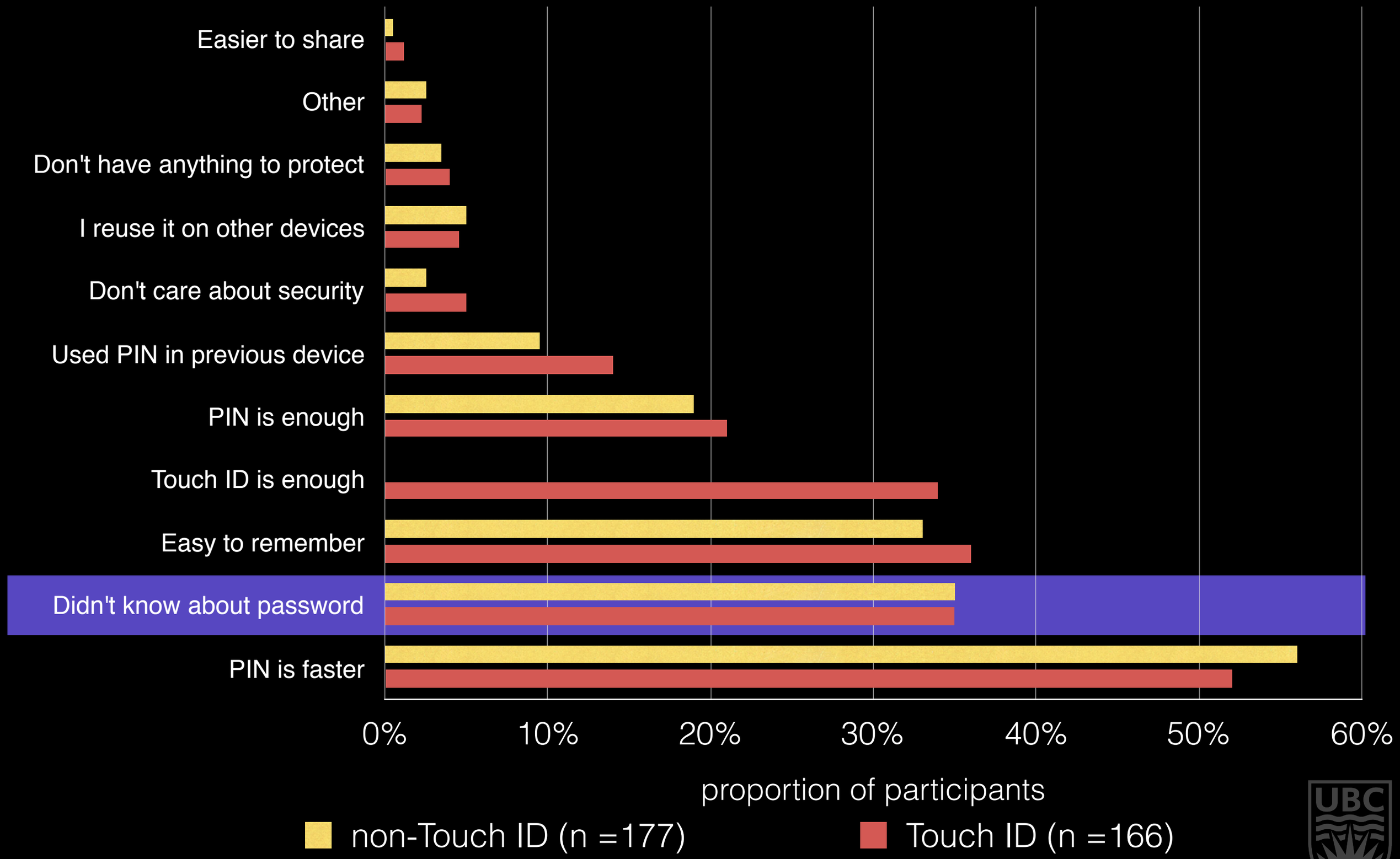
MTurk (n=374)

reasons for using PIN (not pwd)



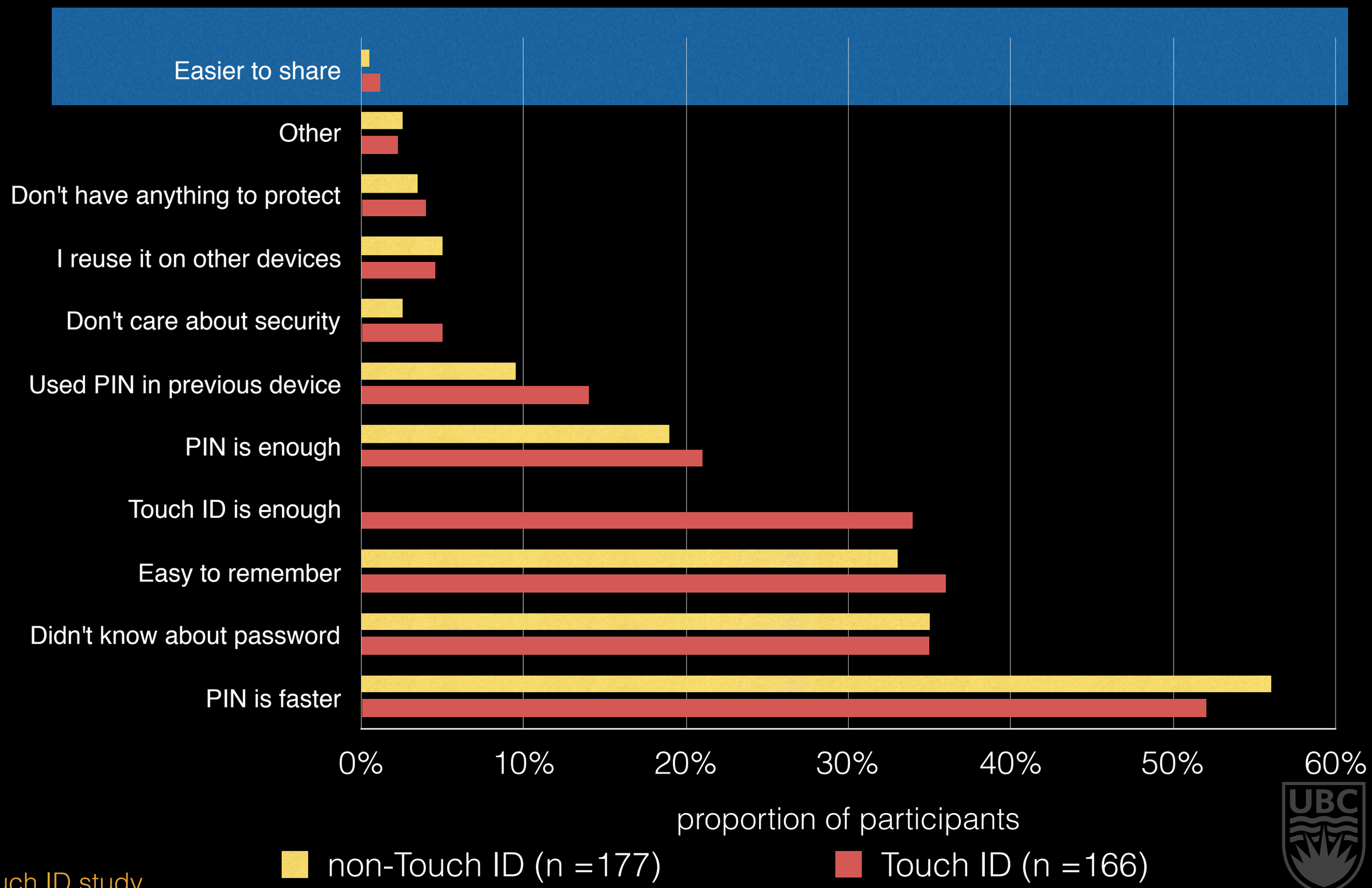
Laboratory for Education and Research in Secure Systems Engineering
(lersse.ece.ubc.ca)

reasons for using PIN (not pwd)

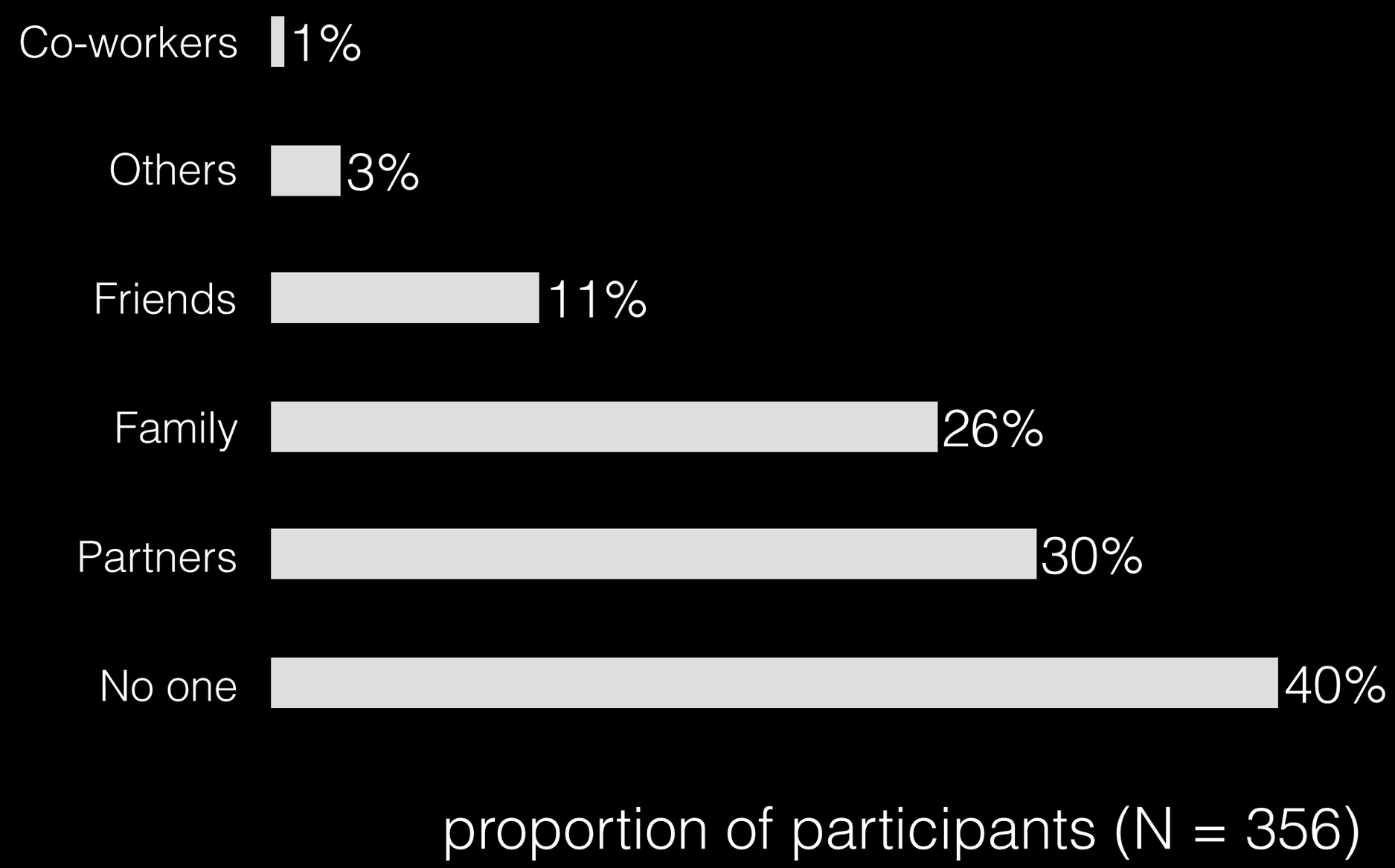


Laboratory for Education and Research in Secure Systems Engineering
(lersse.ece.ubc.ca)

PINs are easier to share



who users share PIN with?



more on phone sharing

[Matthews, Google, CHI ’16]

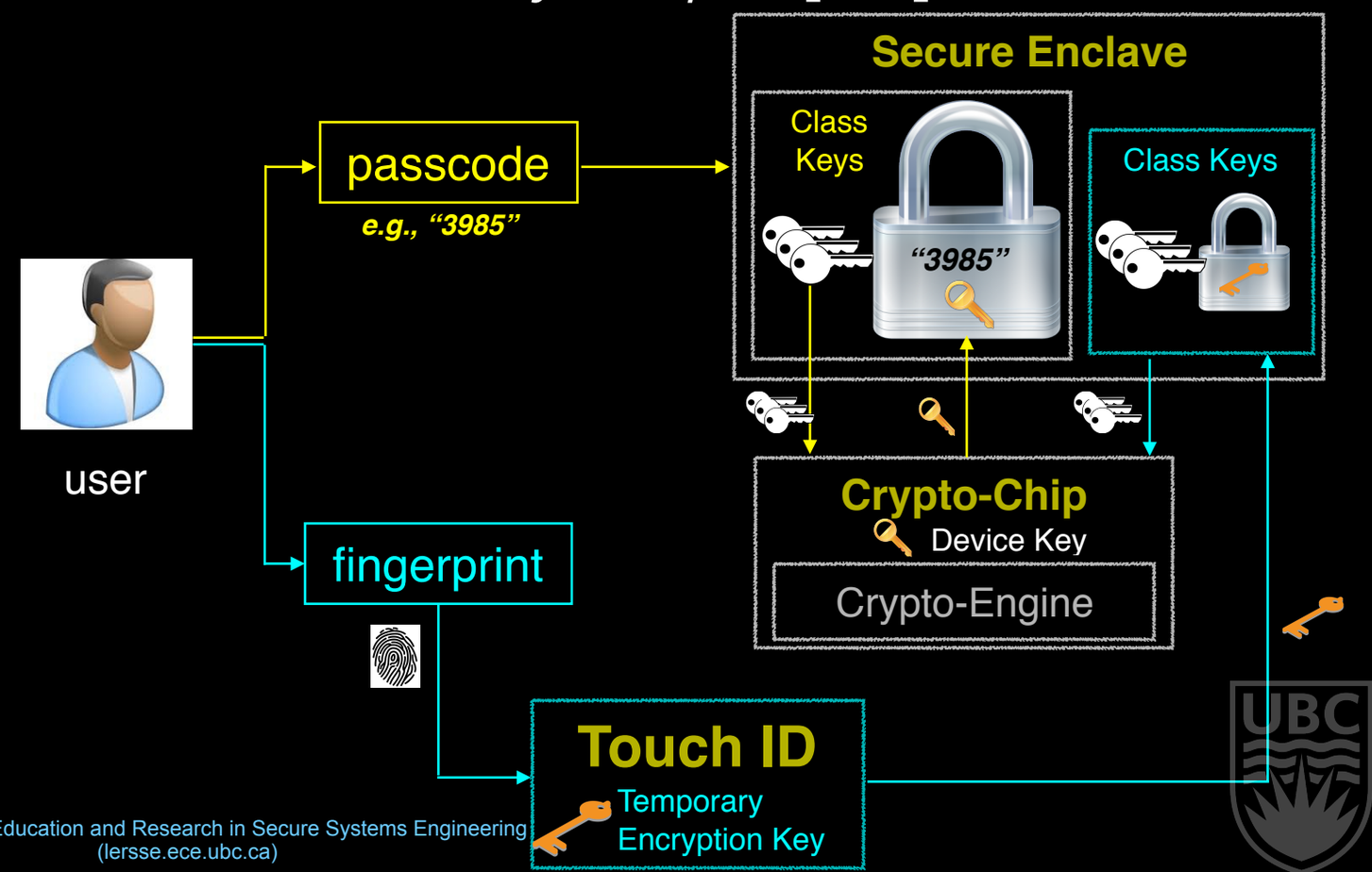
- share mostly with significant others and children
- sharing types
  - borrowing (device but not accounts) for convenience.
  - set up/maintenance (access remaining) to help
  - broadcasting to view content together
  - accidental account sharing
- trust and convenience dimensions

T. Matthews, K. Liao, A. Turner, M. Berkovich, R. Reeder, and S. Consolvo.``**"She'll just grab any device that's closer": A Study of Everyday Device & Account Sharing in Households**.” In Proceedings of CHI ’16, pp. 5921-5932.

confusion about passcode vs. Touch ID

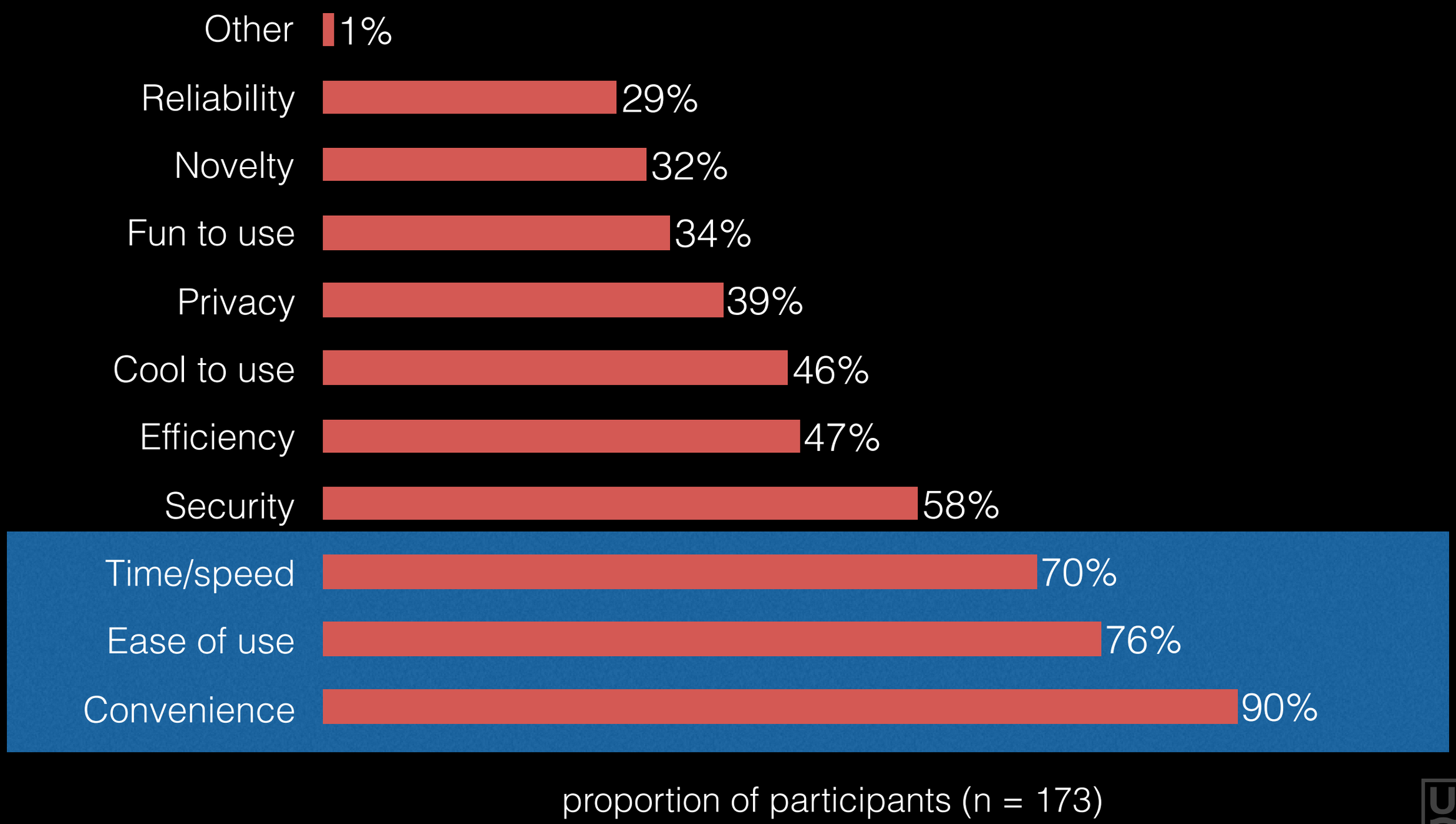
Touch ID itself increases security

> "*I guess Touch ID will protect my phone. They cannot open my phone without my finger. So it will definitely help.*" [P1]



why Touch ID?

reasons for using Touch ID



Laboratory for Education and Research in Secure Systems Engineering
(lersse.ece.ubc.ca)

main findings (1/2)

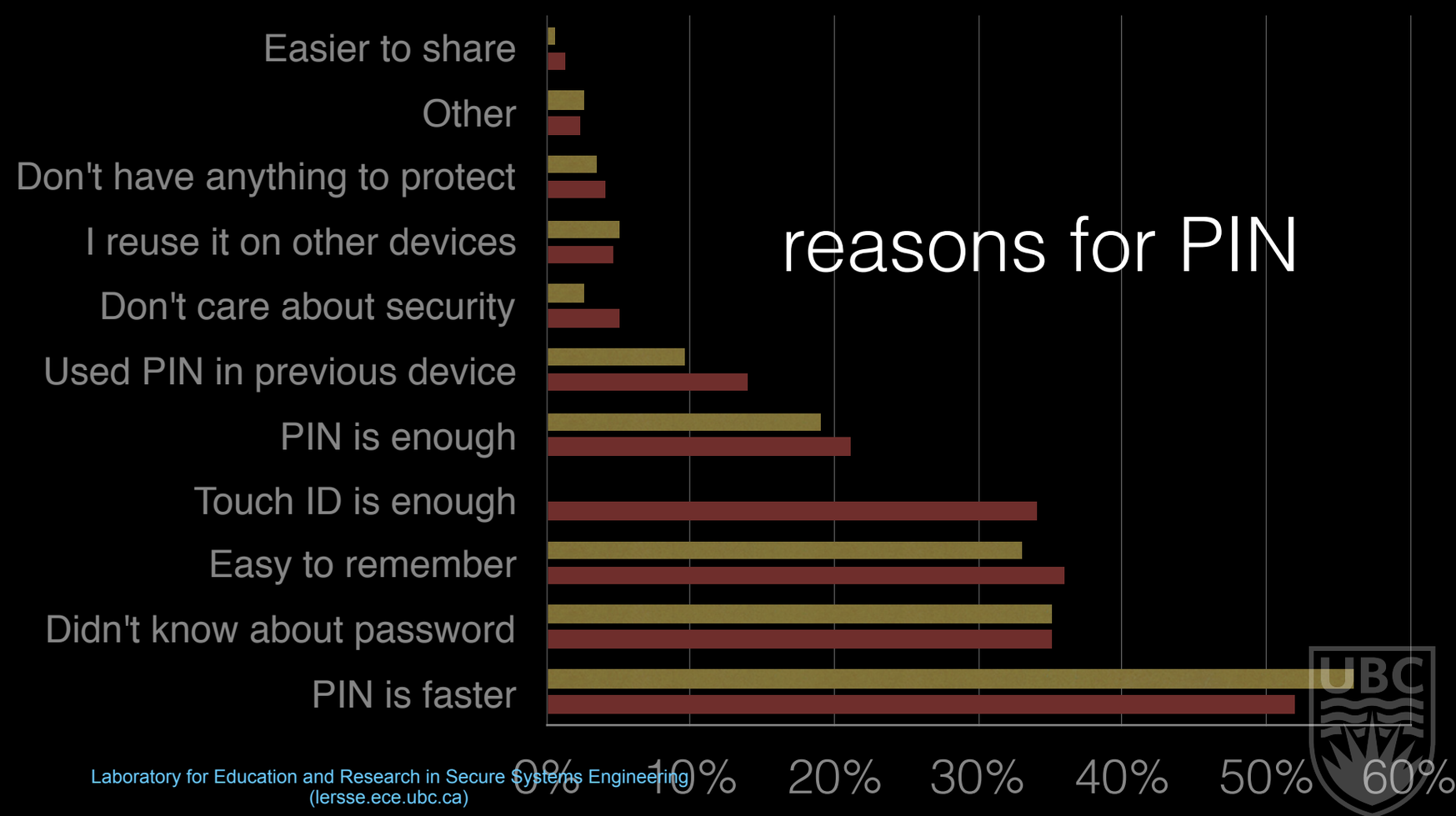
- Users' concerns about strangers and social insiders are comparable
- 1 in 5 Americans engaged in smartphone snooping in past 12 months
- Overwhelming majority of iPhone (but not Android) users lock their devices
- Smartphone locking is likely linked to its value (hardware, data, apps)
- Most sessions are short and involve 1-3 apps
- Usability cost of unlocking methods is crucial

main findings (2/2)

- Touch ID is for convenience
  - no measurable impact of TouchID on passcodes
  - passcodes are weak: 1-2 hours to guess
- PINs vs. passwords
  - usability (e.g., sharing) considerations
  - lack of awareness: set up, salespeople
- unlocking methods need to support device sharing

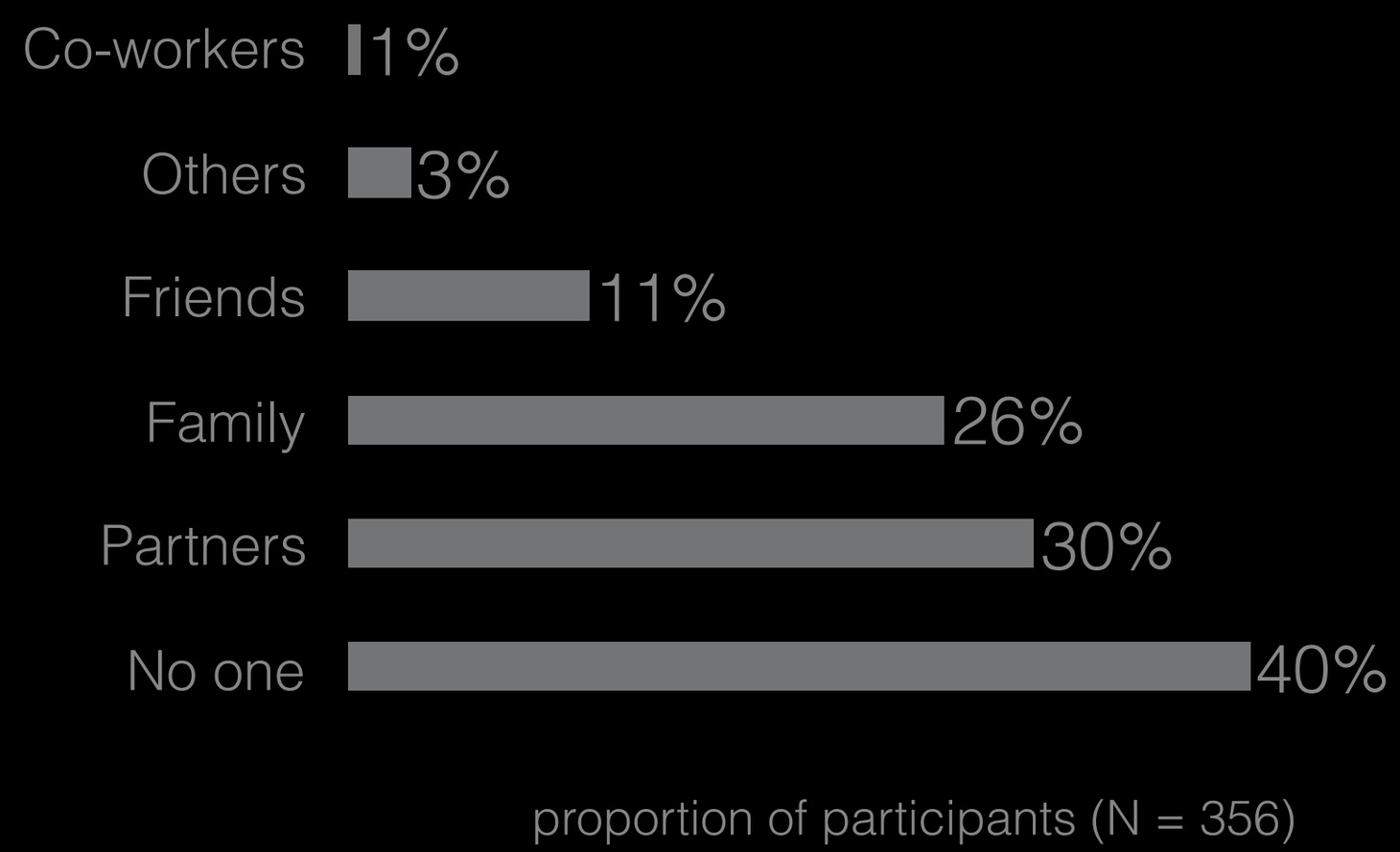
design recommendations: **unlocking secrets**

- stronger than PINs and yet just as memorable
- comparable speed and accuracy



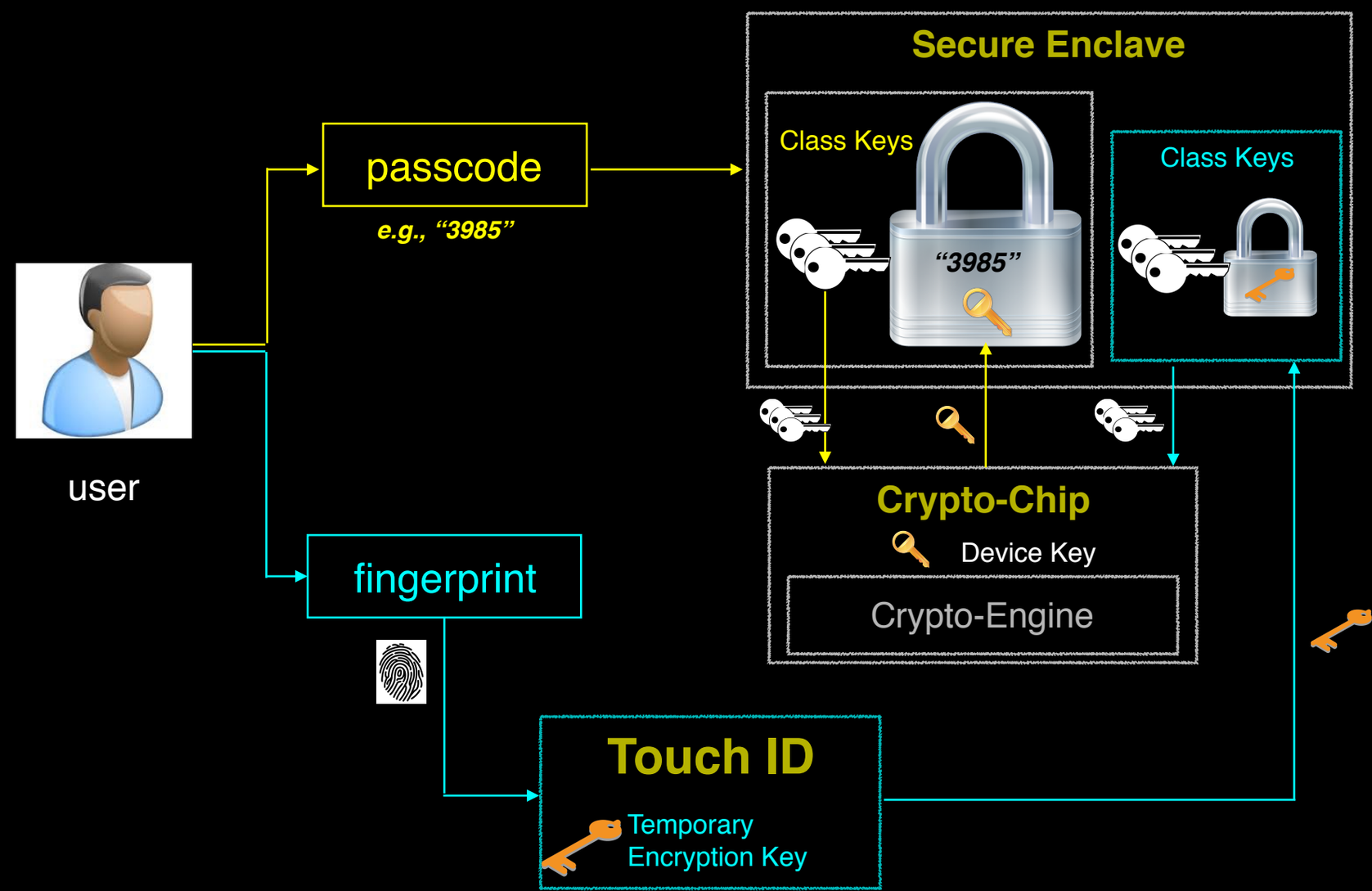
design recommendations

facilitate phone sharing



facilitate contacting owners of lost phones

design recommendations:
better mental model of TouchID+passcode



design recommendations

better feedback on passcode strength

acknowledgements

LERSSE team

- Ildar Muslukhov
- Ivan Cherapau
- Ahmed Mahfouz
- Yazan Boshmaf
- Nalin Asanka

Collaborators

- University of Lisbon
  - Diogo Marques
  - Tiago Guerreiro
  - Luís Carriço
- Nokia Research
  - Cynthia Kuo
  - Jonathan Lester

Smartphone Users' Family, Friends, and Other Enemies

Konstantin (Kosta) Beznosov

a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

Laboratory for Education and Research in Secure Systems
Department of Electrical and Computer Engineering

selected publications

- I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, K. Beznosov, "Understanding Users' Requirements for Data Protection in Smartphones," in Proceedings of ICDE Workshop on Secure Data Management on Smartphones and Mobiles, Washington D.C., USA, 5 April 2012, pp. 228-235.
- I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, and K. Beznosov, "Know Your Enemy: The Risk of Unauthorized Access in Smartphones by Insiders," In Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services (Mobile HCI), August 27 - 30, 2013, Munich, Germany, pp. 271-280.
- A. Mahfouz, I. Muslukhov, K. Beznosov "Android Users in the Wild: Their Authentication and Usage Behaviour" in Pervasive and Mobile Computing, Elsevier, 2016.
- I. Cherapau, I. Muslukhov, N. Asanka, and K. Beznosov, "On the Impact of Touch ID on iPhone Passcodes," in Proceedings of Symposium On Usable Privacy and Security (SOUPS), Ottawa, Canada, July 22-24, 2015, pp. 257-276.
- (distinguished paper award) D. Marques, I. Muslukhov, T. Guerreiro, L. Carriço, K. Beznosov, "Snooping on Mobile Phones: Prevalence and Trends" in Proceedings of Symposium On Usable Privacy and Security (SOUPS), Denver, CO, USA, June 22-24, 2016, pp. 159-174.