Neither Access nor Control:

A Longitudinal Investigation of the Efficacy of User Access-control Solutions on Smartphones

Masoud Mehrabi-Koushki

(Presenter)

Yue Huang

Julia Rubin

Konstantin Beznosov

THE UNIVERSITY OF BRITISH COLUMBIA

ece Electrical and Computer Engineering

Phone security is becoming important

- More capable phones

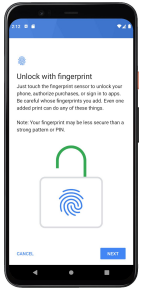
- Sensitive data/services [1] → More damage if unauthorized access [2]

- **Physical security** → important aspect
  - Attacker has physical access

[1] Egelman S, Jain S, Portnoff RS, Liao K, Consolvo S, Wagner D. *Are You Ready to Lock?* In ACM Conference on Computer and Communications Security (CCS), 2014.
[2] Marques D, Muslukhov I, Guerreiro T, Beznosov K, Carriço L. *Snooping on Mobile Phones: Prevalence and Trends.* In Symposium on Usable Privacy and Security (SOUPS), 2016.

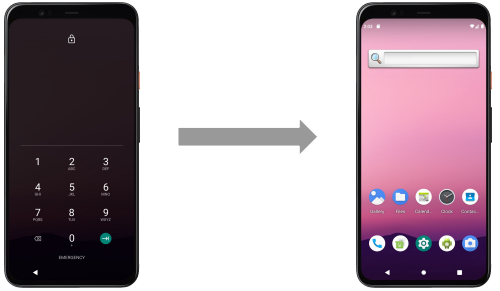
Physical security involves two systems

- **Authentication**
  - **Confirm user identity**
  - *Incumbent*: Explicit authentication [1]



  - Investigated in prior work [3][4]

- **Access control**
  - **Control what user can do**
  - *Incumbent*: All-or-nothing [2]



[1] Mahfouz A, Muslukhov I, Beznosov K. *Android users in the wild: Their authentication and usage behavior*. Pervasive and Mobile Computing. 2016.
[2] Hayashi E, Riva O, Strauss K, Brush A, Schechter S. *Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications*. In Symposium on Usable Privacy and Security (SOUPS), 2012.
[3] Mehrabi Koushki M, Obieh BO, Huh JH, Beznosov K. *On Android Users' Perception of Smart Lock for Android*. In ACM Conference on Human-Computer Interaction with Mobile Devices and Services (MobileHCI), 2020.
[4] Mehrabi Koushki M, Obieh BO, Huh JH, Beznosov K. *On Smartphone Users' Difficulty with Understanding Implicit Authentication*. In ACM CHI Conference on Human Factors in Computing Systems (CHI), 2021.

All-or-nothing dissatisfies users

➔ No Task-sensitivity

- ***Reading book*** → Unnecessary protection [1]
- ***Financial ops*** → Insufficient protection [1]

➔ No Phone-sharing

- Lack of control over sharees → Snooping [2]

[1] Hayashi E, Riva O, Strauss K, Brush AJB, Schechter S. *Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications*. In Symposium on Usable Privacy and Security (SOUPS), 2012.
[2] Marques D, Muslukhov I, Guerreiro T, Beznosov K, Carriço L. *Snooping on Mobile Phones: Prevalence and Trends.* In Symposium on Usable Privacy and Security (SOUPS), 2016.

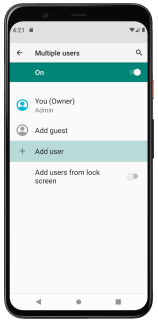
Alternatives are proposed, but not compared

- **Task-sensitivity**
  - **Commercial**

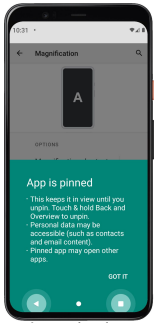
Lock screen access

  - App- [1] or Task- [2] level
  - Context-based [3]

- **Phone-sharing**
  - **Commercial**



Profile switching



App pinning

  - DiffUser [4]
  - xShare [5]

[1] Riva O, Qin C, Strauss K, Lymberopoulos D. *Progressive authentication: deciding when to authenticate on mobile phones*. In USENIX Security Symposium, 2012.
[2] Hayashi E, Riva O, Strauss K, Brush AJB, Schechter S. *Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications*. In Symposium on Usable Privacy and Security (SOUPS), 2012.
[3] Hayashi E, Das S, Amini S, Hong J, Oakley I. *Casa: context-aware scalable authentication*. In Symposium on Usable Privacy and Security (SOUPS). 2013.
[4] Ni X, Yang Z, Bai X, Champion AC, Xuan D. *Diffuser: Differentiated user access control on smartphones*. In International Conference on Mobile Adhoc and Sensor Systems, 2009.
[5] Liu Y, Rahmati A, Huang Y, Jang H, Zhong L, Zhang Y, et al. *xShare: supporting impromptu sharing of mobile phones*. In international conference on Mobile systems, applications, and services (Mobisys), 2009.

Research Questions:

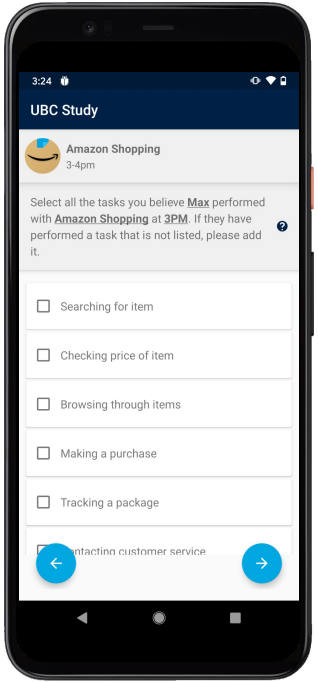
- **RQ1 {users' needs}**: What **tasks** do smartphone users perform on their phones? What are their **sharing preferences** for the tasks?

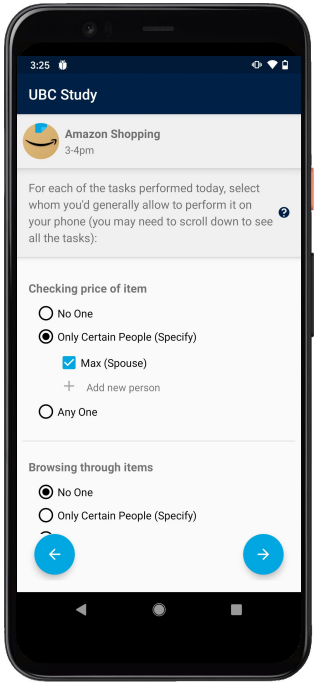
- **RQ2 {comparing solutions}**: To what extent, in terms of **False Positive Rate (FPR)** and **False Negative Rate (FNR)**, do all-or-nothing and the alternative solutions meet the users' needs? How do they compare in **Configuration Size Rate (CSR)**?

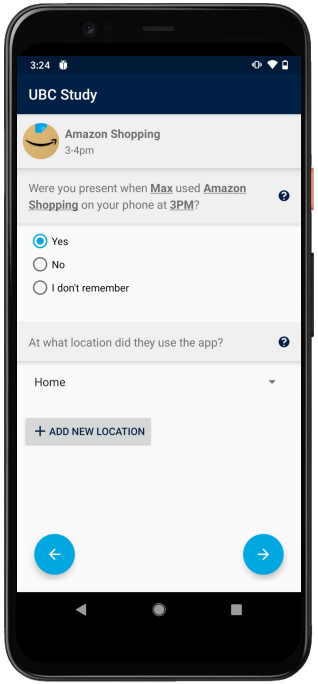
- **RQ3 {sharing context}**: How **consistent** are **contextual factors** (e.g., with whom the phone is shared, where, and for what purpose) across phone-sharing events?

We conducted a longitudinal diary study

- **Custom Android app**
  - **55** MTurk participants
  - > **30** days
- **Daily diaries**
  a. Tasks performed
  b. Task sharing preferences
  c. Sharing context
- **Data analysis**
  - Qualitative coding
  - Descriptive statistics
  - Chi-squared tests

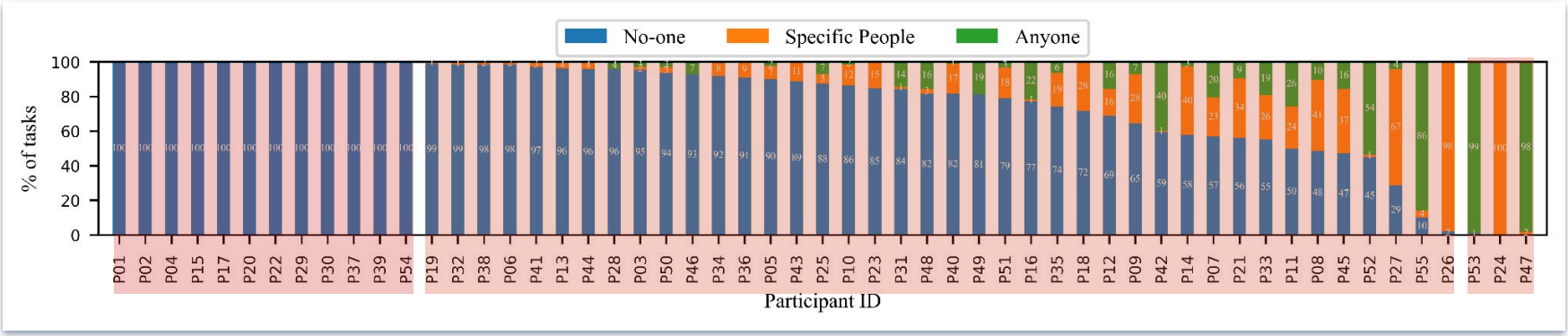






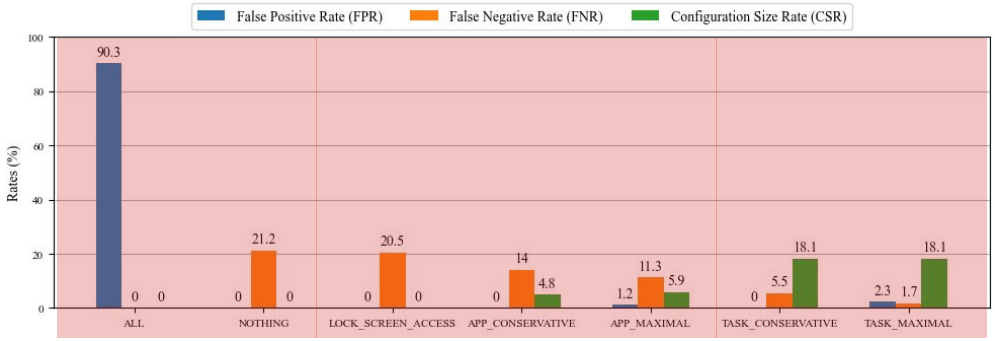
RQ1 {users' needs}:
We observed diverse tasks, complex needs

- **Lots of tasks**
  - **1,149** tasks with **571** apps
  - **74** per person, **2** per app
- **Complex needs**
  - **24%** Specific people, **19%** Anyone
  - Individual differences

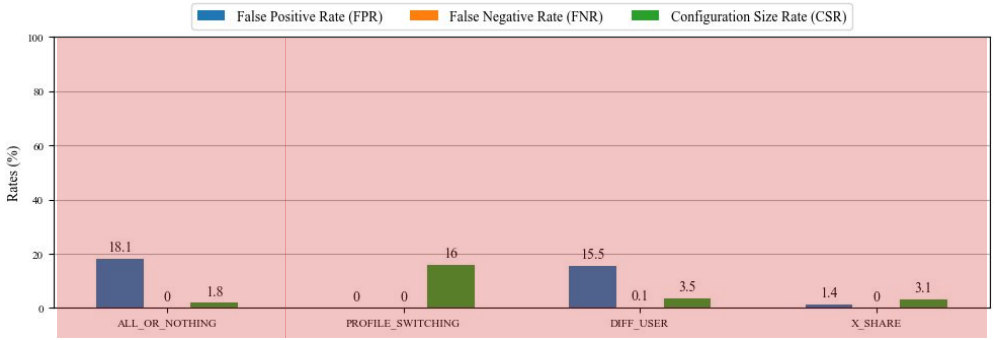


RQ2 {comparing solutions}:
App-level task-sensitivity & session-based phone sharing perform best

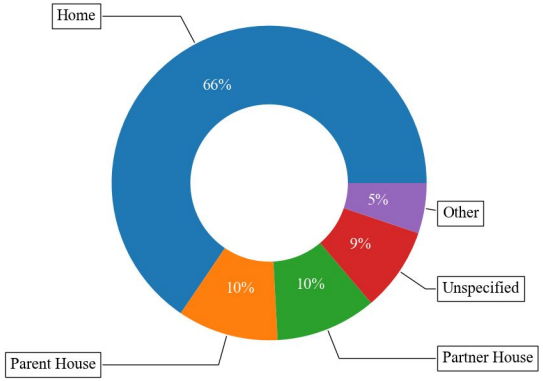
- **Task-sensitivity**
  - ***ALL-or-NOTHING:*** inefficient
  - ***Commercial***: ineffective
  - ***App-level***: best balance
  - ***Task-level***: effective, high config

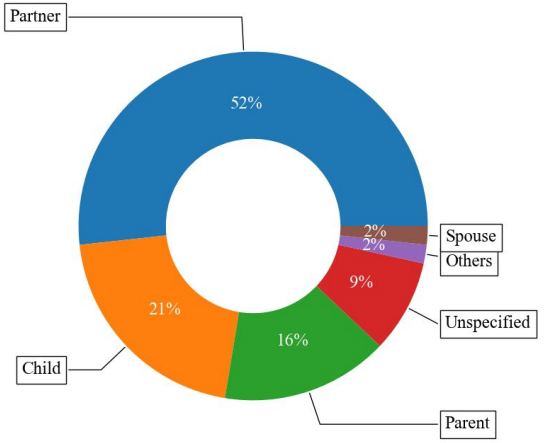


- **Phone-sharing**
  - ***All-or-NOTHING:*** inefficient
  - ***Commercial***: effective, high config
  - ***Proposed***: xShare best



RQ3 {sharing context}:
Context is fairly consistent in phone sharing





- **Location**: 86% at home (own or partner)
- **Sharee**: 89% with immediate family

We provided quantitative evidence for:

- **Users' access control needs are complex**
  - Many tasks, scattered sensitivity distribution
  - Preferences vary by **functionality** and **personality**

- **Implemented solutions are suboptimal**
  - **All-or-nothing** → 90% FPR, 21% FNR
  - **Lock screen access** → only 1% improvement

- **Some proposed solutions seem promising**
  - **Task-sensitivity** → app-level
  - **Phone-sharing** → session- and context-based

Thank you for listening!

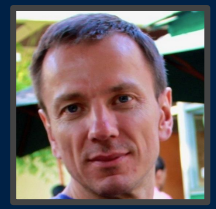
Please feel free to contact us if you have any questions.

Masoud is on the job market (smartphone or usable security positions). Please contact him if you have an opening.

Masoud Mehrabi-Koushki
mehrabi@ece.ubc.ca

Yue Huang
huang13i@ece.ubc.ca

Julia Rubin
mjulia@ece.ubc.ca



Konstantin Beznosov
beznosov@ece.ubc.ca