Sharing without Scaring:
Enabling Smartphones to Become Aware of Temporary Sharing

Jiayi Chen[1], Urs Hengartner[1], Hassan Khan[2]

University of Waterloo[1], University of Guelph[2]

UNIVERSITY OF WATERLOO

CrySP
Cryptography, Security, and Privacy Research Group
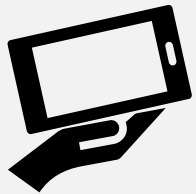
UNIVERSITY of GUELPH

IMPROVE LIFE.

Temporary Device Sharing

Motivation
- Helping
- Convenience
- Social purposes
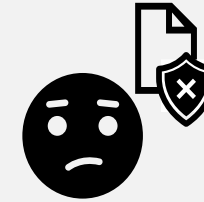
Sharing practice
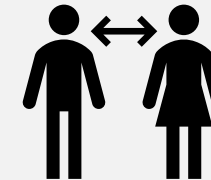- Supervision
- Sharing protection
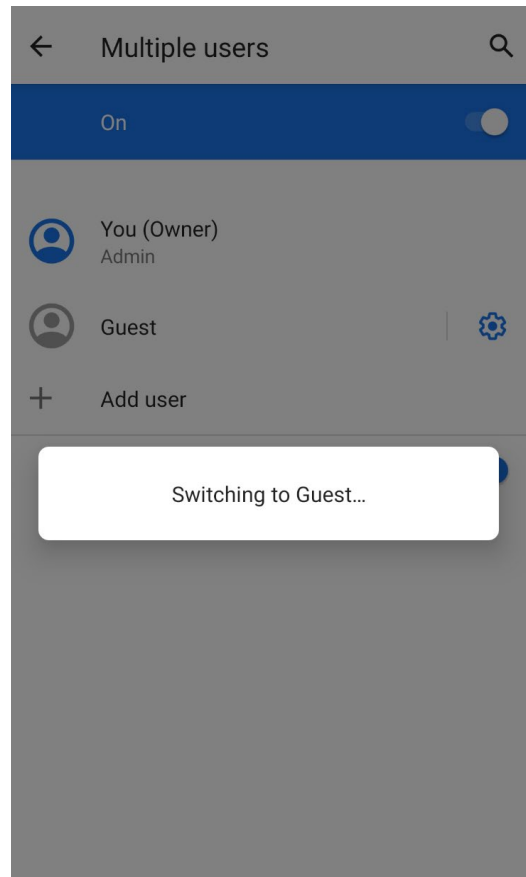
Owner **Sharee**

Privacy concern
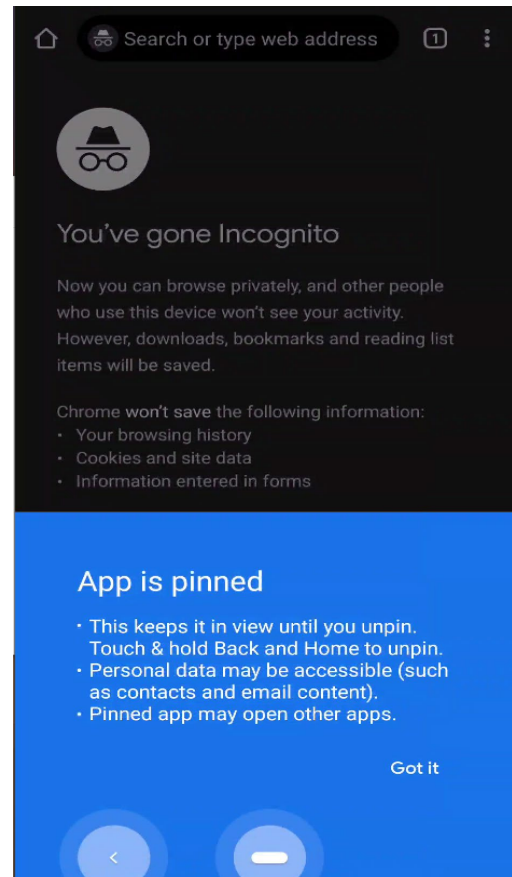- Personal data
- Sensitive operations

Social implication
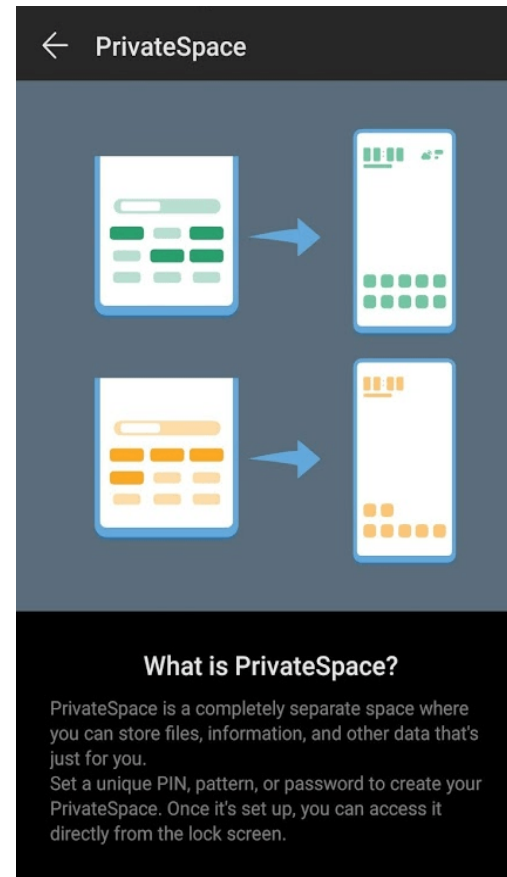- Trust
- Relationship
- Culture

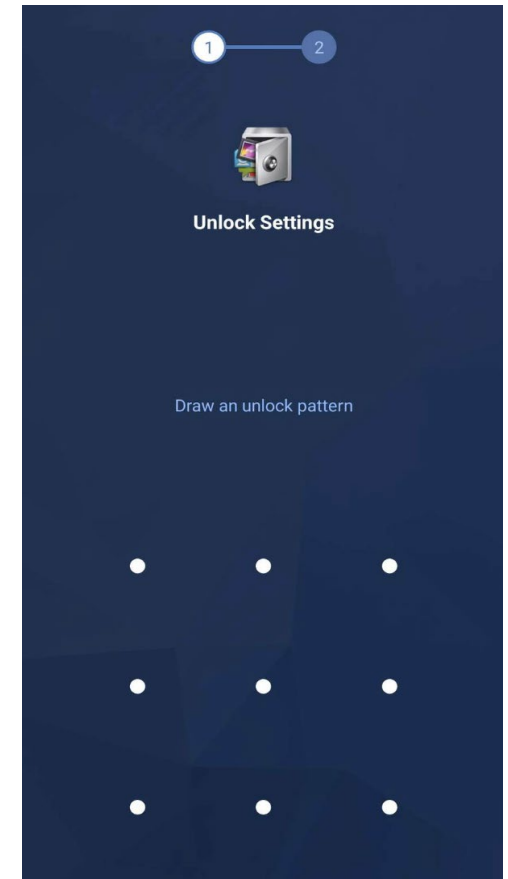# Device Sharing Protection Solutions

Guest account

App pinning

Vault

App lock

Owner's Failure to Enable Sharing Protection
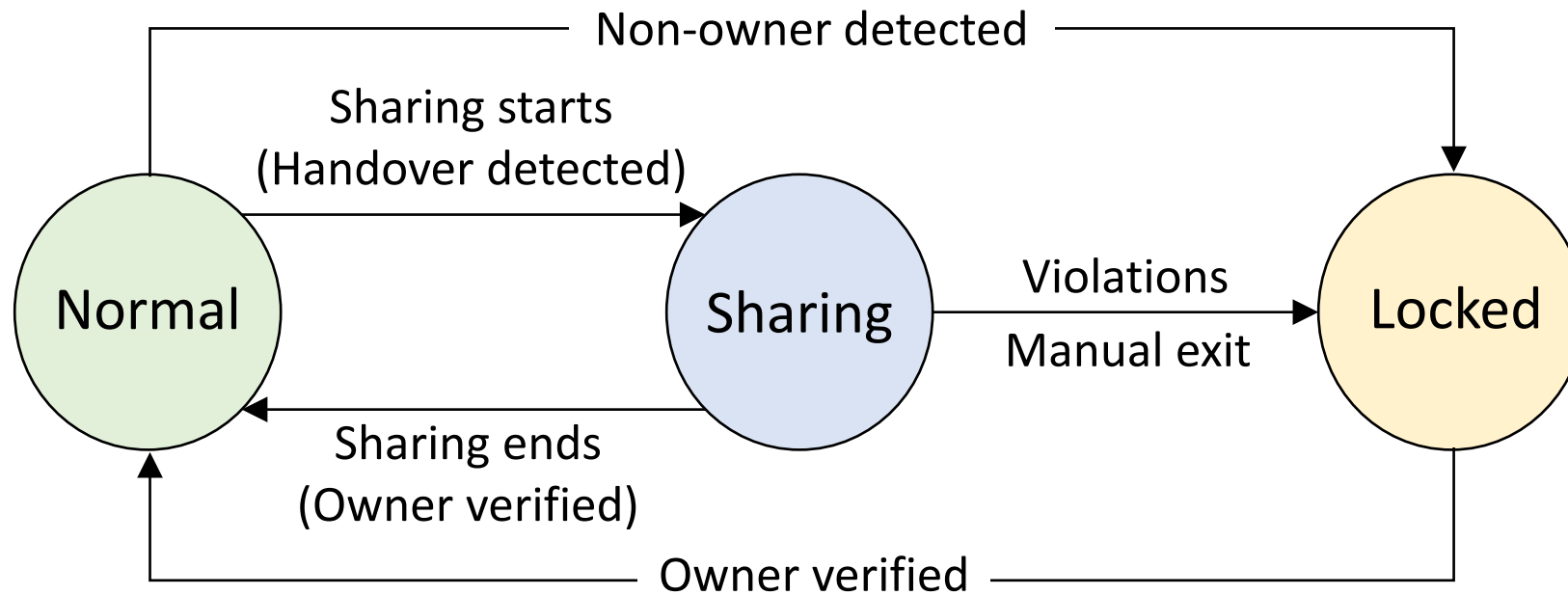
Forgetfulness

Lack of risk perception

Avoiding signaling mistrust

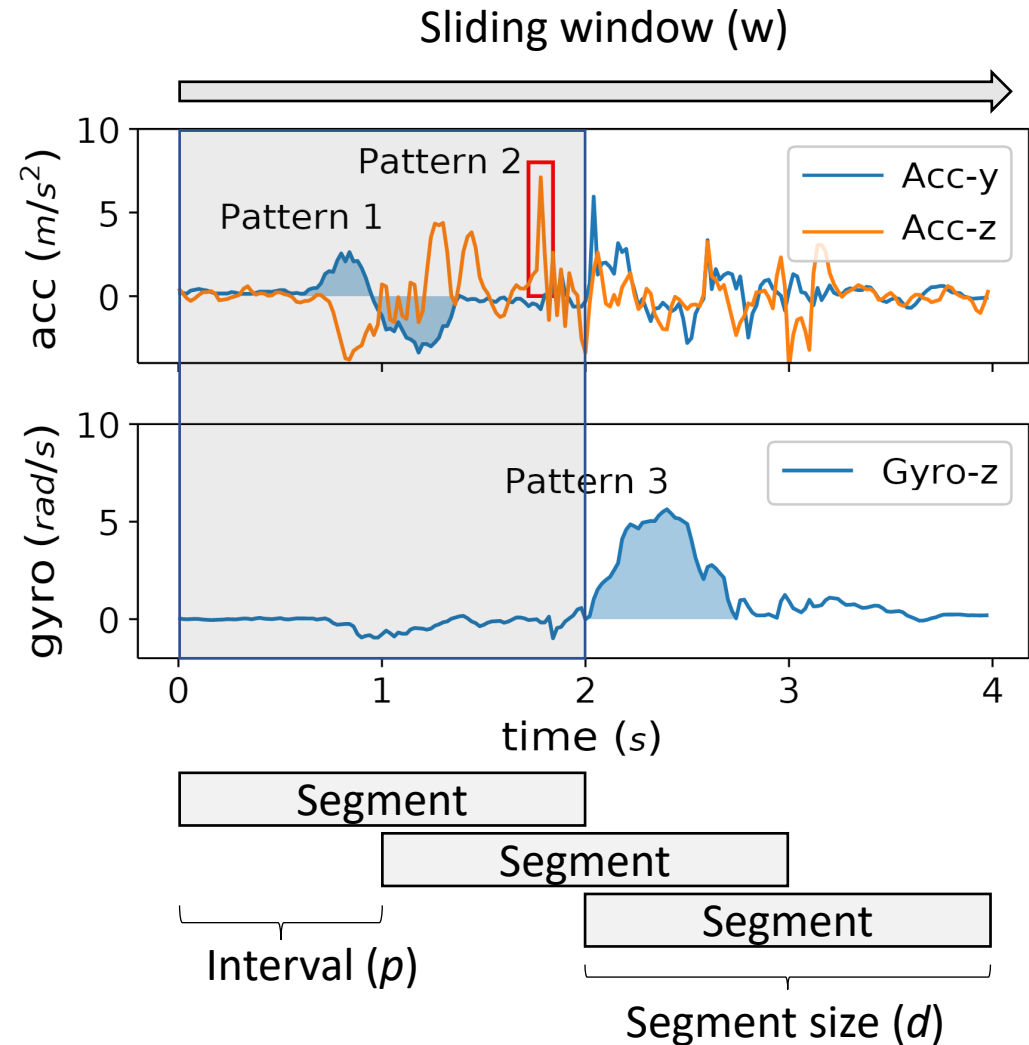**Need for <u>proactive</u> device sharing protection solution**

Device Sharing Awareness (DSA)

*Determine **when to** activate and deactivate sharing protection*

Sharing Gesture Detection

- Start a sharing event

- Handover gesture
  - Owner handing device to sharee
  - Distinguishing handover from other common movements

- Pre-trained cross-user model

- Adaptive sensing

Owner Detection

- End a sharing event

- Behavioral biometrics
  - Implicit Authentication (IA)
  - User recognition by how they interact with device
  - E.g., touch patterns, keystroke dynamics

- Handle exceptions
  - Prevent unauthorized access
  - Handle false sharing detection

Owner's strokes   Sharee's strokes
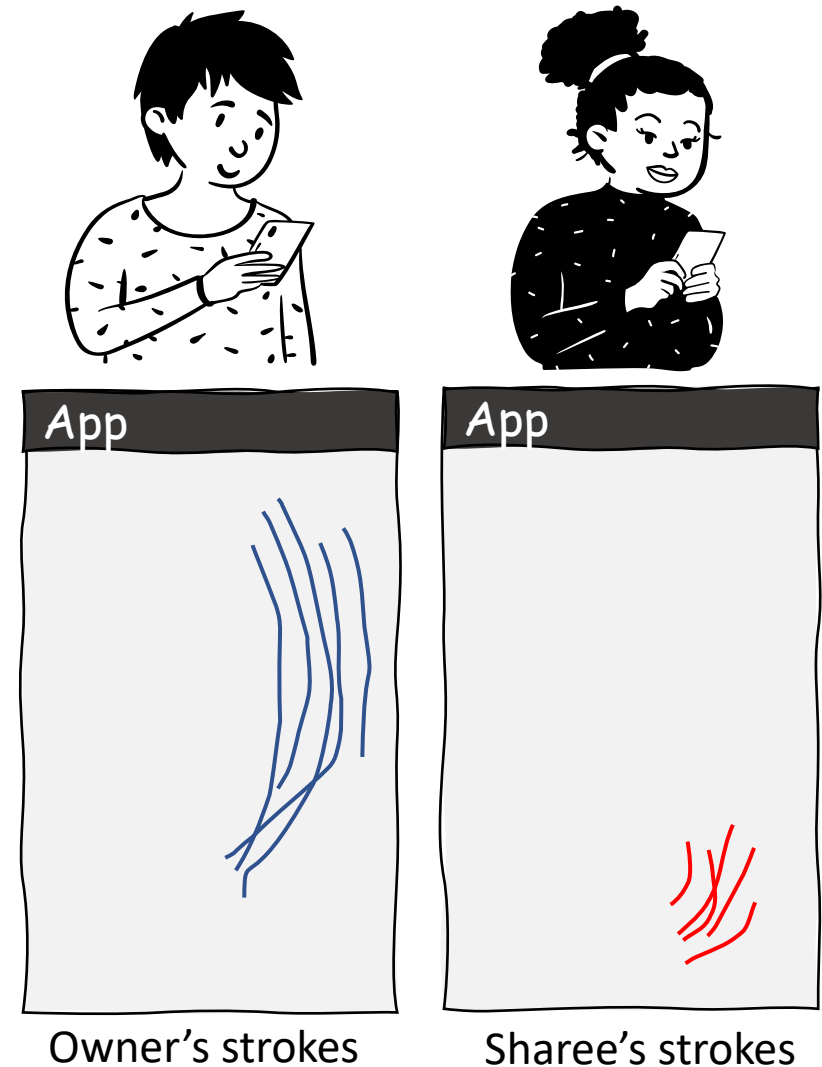
Implementation

- DSA Service
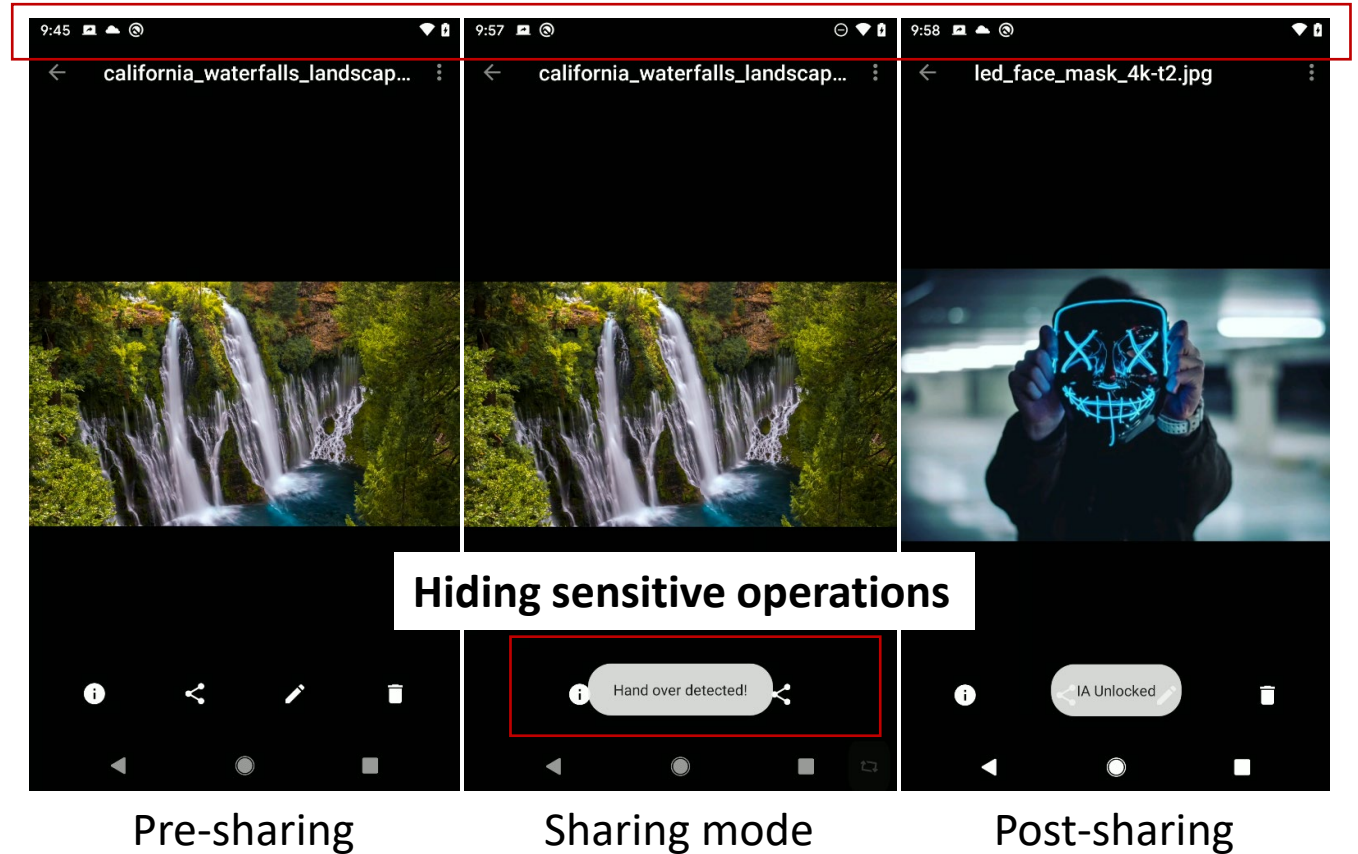 - Sharing detection
  - App-level access control
  - Notification management
- Interaction with apps
  - Tracking the current app
  - Notifying apps of device sharing

Hiding sensitive notifications

Hiding sensitive operations

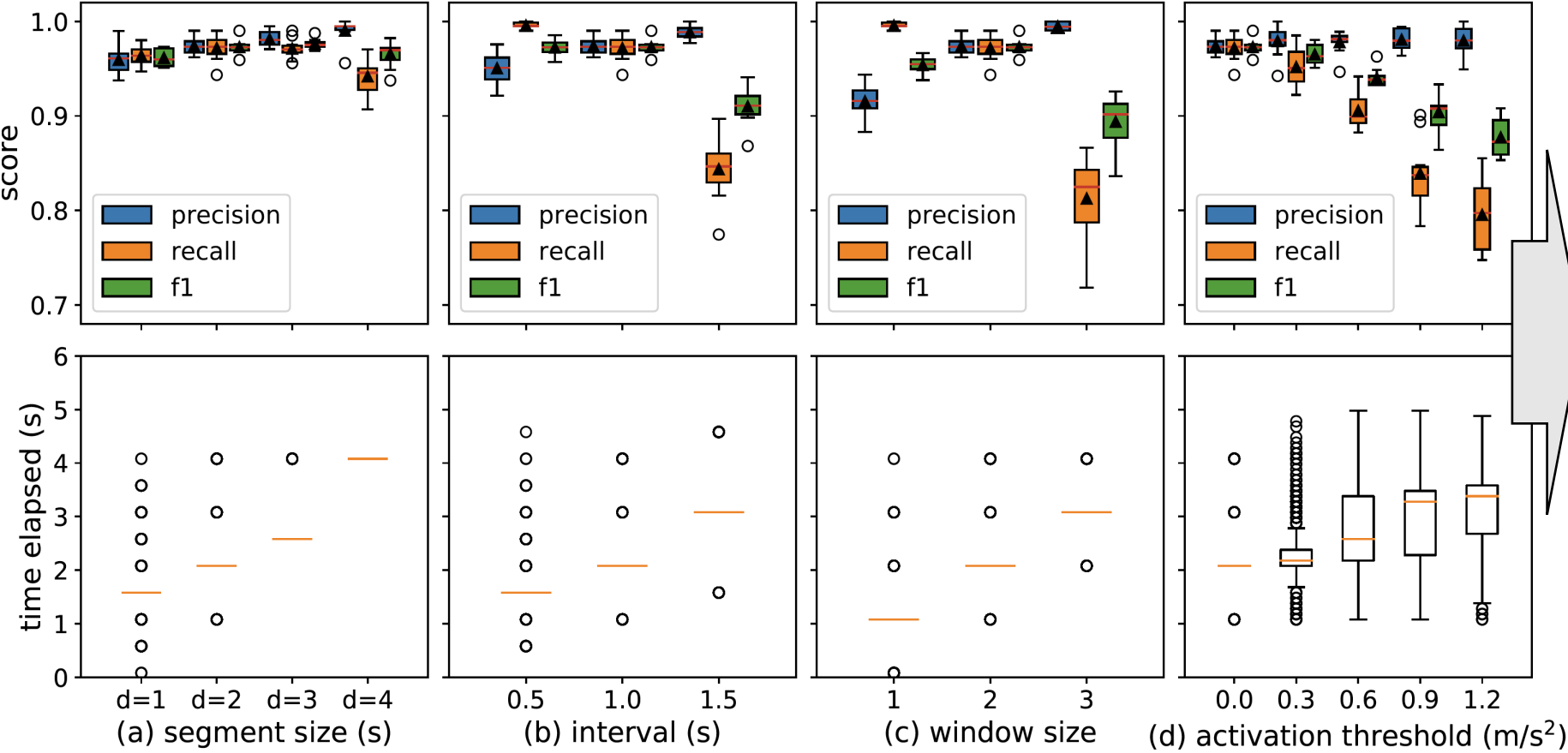Pre-sharing   Sharing mode   Post-sharing

Evaluation Setup

- Handover detection evaluation
  - 18 participants, 5 device models
  - 2044 handover, 1737 non-handover data clips
  - Evaluating cross-user, cross-device detection accuracy
  - Building a pre-trained model with tuned hyperparameters

- Sharing handling evaluation
  - 10 participants, 50 sessions
  - Webpage sharing tasks
  - Adopting Touchalytics IA [1] for owner detection
  - Evaluating how DSA handles complete device sharing events

[1] Frank, Mario, et al. "Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication." IEEE transactions on information forensics and security 8.1 (2012): 136-148.
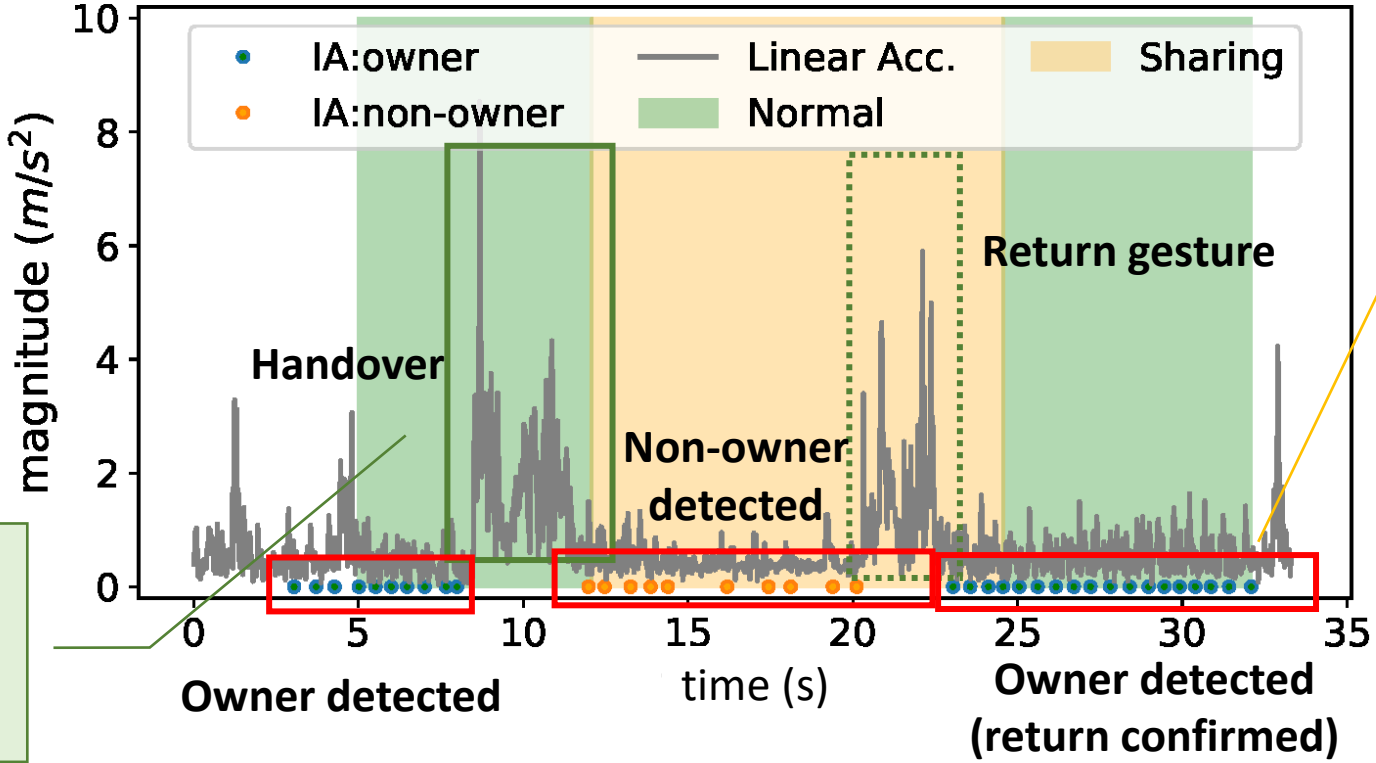
Handover Detection Results

Best settings
segment size = 2s
interval = 1s
window size = 2
threshold = 0.3 m/s^2

Performance
precision: 0.98
recall: 0.95
reaction time: 2.33s

Device Sharing Trace

DSA started sharing mode right after detecting a handover

DSA ended sharing mode only after confirming owner's identity

DSA automatically handled 41/50 sessions without exceptions.
7/9 sessions were corrected by owner detection.

Conclusion

- We proposed DSA to proactively detect and handle temporary device sharing.

- We implemented DSA Service on Android for demonstration.

- A user study showed the effectiveness of DSA in handover gesture detection and sharing handling.

- Data and source code are available at: https://github.com/cryspuwaterloo/DSA-Framework.

- Future avenues
  - Extending sharing gesture detection under more contexts
  - Conducting a long-term user study to evaluate user acceptance of DSA

- Thank you for listening! Email: jiayi.chen@uwaterloo.ca