Human-Computer Interaction and Security Engineering Lab Secure Systems Group, Aalto University

Amel Bourdoucen, Janne Lindqvist

## Understanding Privacy and Security of Mobile Ecosystems

Figure 1: Flow diagram illustrating mixed methods approach



Analysis of app functionalities and privacy configurations of 8 apps.

## What is a Mobile Ecosystem?

A mobile ecosystem consists of units (e.g., devices)

Safari, Siri, Family Sharing, Find My, Touch ID, Location Services, iMessage and Facetime. Online Screening Survey (N=67) Adults located in Finland (N=15) English speakers, and have used at least three apps listed. that interact with each other through information exchange.

- Mobile ecosystems provide convenience, ease of use and a cohesive experience.
- Challenges with Mobile Ecosystems
- Growth in complexity.
- Certain privacy configurations of default apps are only prompted once during initial device setup.
- Prior work suggested that users often have misconception about data sharing on smart phone apps [1,2].

## **Research Study Findings**

Participants were confused about what happened

(a) Setup Process of devices
(b) Storage of personal information
(c) Synchronisation of personal information
(d) Disabling Features
Users perform practical tasks (e.g., disabling privacy configurations) on their devices.

to their information.

- Participants did not know how to disable many privacy configurations.
- Location Tracking can induce trust issues in family relationships.

[1] J. Tan, K. Nguyen, M. Theodorides, H. Negr.n-Arroyo, C. Thompson, S. Egelman, and D. Wagner, "The effect of developer-specified explanations for permission requests on smartphone user behavior," CHI '14. New York, USA: Association for Computing Machinery, 2014, p. 91–100.

[2] R. Balebako, J. Jung, W. Lu, L. F. Cranor, and C. Nguyen, ""little brothers watching you": Raising awareness of data leaks on smartphones," SOUPS '13. New York, NY, USA: Association for Computing Machinery, 2013.

TouchID	TouchID	Complete
Use your fingerprint in place of your passcode or Apple ID password for purchases.	Use your fingerprint in place of your passcode or Apple ID password for purchases.	Touch ID is ready.
Setup Touch ID later		

Example case When enabling Touch ID, users are unable to read where their finger print information is stored upon initially setting up their device. Apple claims that finger print information is never stored on Apple's servers.



Figure 2: Setup process of Touch ID feature (fingerprint scanner) for Apple devices



**Aalto University**