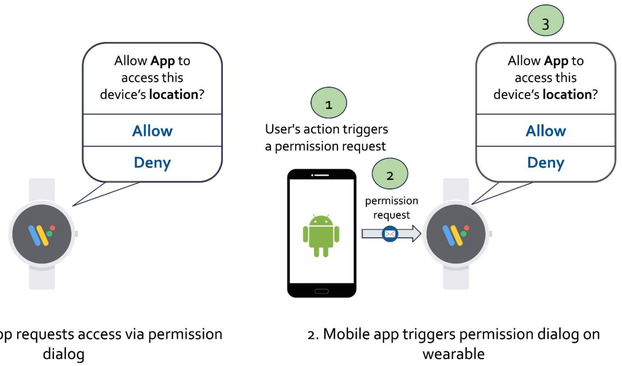
Wear's my Data? Understanding the Cross-Device Runtime Permission Model in Wearables

Doguhan Yeke†, Muhammad Ibrahim†, Güliz Seray Tuncay‡, Habiba Farrukh†¶, Abdullah Imran†, Antonio Bianchi†, Z. Berkay Celik†

†Purdue University, ‡Google, ¶University of California, Irvine

Introduction

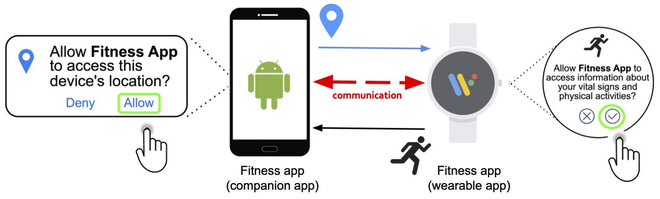


1. Wearable app requests access via permission dialog

2. Mobile app triggers permission dialog on wearable

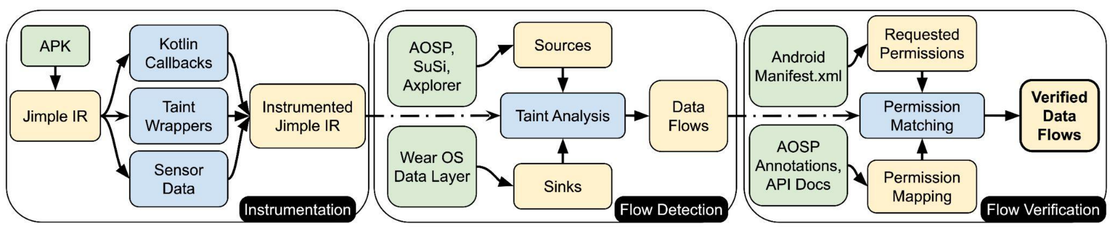
Understanding the privacy implications of the **dual permission model** adopted by mobile and wearable ecosystems to govern user data by two independent permission models.

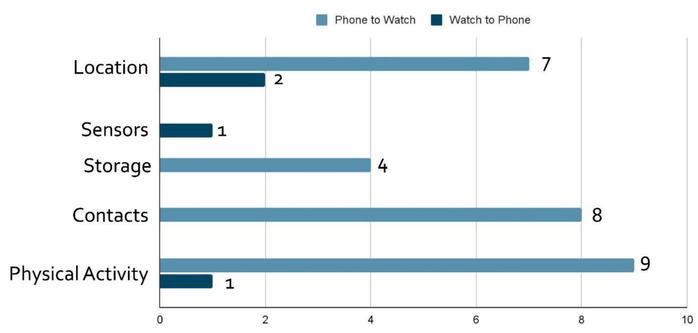
Motivation



If permission is granted on one device, data becomes accessible on both devices, which can violate user privacy if they expected data access to be restricted to just one device.

FlowFinder





Out of 150 apps, 28 have cross-device data flows!

How Apps Inform Users

Do platform/apps properly inform users about cross-device data flows?

App descriptions

2 **apps** mentioned data transfers across devices in their app descriptions among all the apps.

Privacy Policies

1 app **explicitly stated** which data is transferred and provided reasons for the transfers

10 apps **did not clarify** if data is transferred across devices

12 apps **denied** any data transfers across devices

5 apps either **did not disclose** how they use data or **did not have** a privacy policy.

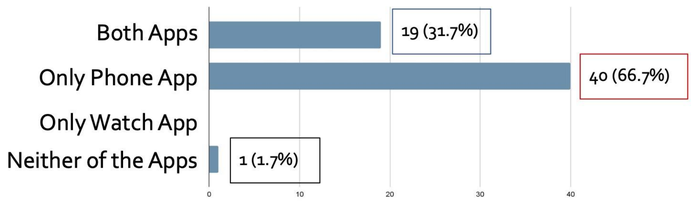
User Study

Semi-structured interviews

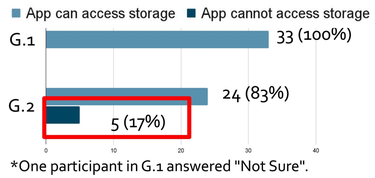
63 Android and/or WearOS users

- **RQ1** How do users perceive permissions to work in the existence of cross-device data flows?
- **RQ2** Can an adversary misguide users into unknowingly granting access to sensitive data?

- Which app(s) can access phone's location when you grant the permission on phone, but deny it on watch?



- Do you think the phone app can access files, photos and videos?



*One participant in G.1 answered "Not Sure".

% of participants who mistakenly believe that the app cannot access storage after seeing the redirection prompt increases from 0% in G.1 to 17% in G.2.

Takeaway:

- Most participants are unaware of cross-device data flows!
- Cross-device permission phishing can be effective!

Conclusion

- Via taint analysis, we showed cross-device sensitive data flows between the wearable app and its companion app.
- We assessed users' mental models on permissions on wearables via in-lab user study.
- We conducted preliminary analysis on other wearables.
- We proposed potential countermeasures.

References

[1] Doguhan Yeke, Muhammad Ibrahim, Güliz Seray Tuncay, Habiba Farrukh, Abdullah Imran, Antonio Bianchi, and Z. Berkay Celik. "Wear's my Data? Understanding the Cross-Device Runtime Permission Model in Wearables." In 2024 IEEE Symposium on Security and Privacy (SP)