Smartwatches and Fitness trackers: Cyberphysical Privacy and Security Threats

IoT and Security

Henrik Strangalies

Institute of Computer Science
Freie Universität Berlin

Motivation behind Smartwatches, Fitness-Trackers and Wearables

The popularity of wearable devices is **growing exponentially** with consumers using these for a variety of service:

- Used to pay in stores.
- Tracking health.
- Display messages/emails.
- Control smart homes.

Motivation behind Smartwatches, Fitness-Trackers and Wearables

The popularity of wearable devices is **growing exponentially** with consumers using these for a variety of service:

- Used to pay in stores.
- Tracking health.
- Display messages/emails.
- Control smart homes.

In a nutshell

Wearable devices make lives more convenient and healthier.

Security and Privacy Threats

As this market continues to grow, these devices will become increasingly vulnerable to cyber-attack and can pose **security** and **privacy** risks:

- Data collection
- Data transfer between wearable device and phone
- Third-party companies
- Location-based threats
- Accelerometer

Width coverage

Surveys to Security/Privacy risks of wearable devices:

- A Survey of Wearable Devices and Challenges, Suranga Seneviratne et al., Published 26 July 2017, IEEE Communications Surveys & Tutorials
- A Survey of Privacy Vulnerabilities of Mobile Device Sensors, Paula Delgado-Santos et al., 2021, ACM Computing Surveys (CSUR)

Security Threats/Password Leaks:

- MoLe: Motion Leaks through Smartwatch Sensors, He Wang et al., Published 7 September 2015, Proceedings of the 21st Annual International Conference on Mobile Computing and Networking
- When Good Becomes Evil: Keystroke Inference with Smartwatch, Xiangyu et al., Published 12 October 2015, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security

Privacy threats:

- Privacy implications of accelerometer data: a review of possible inferences, Jacob Leon Kröger et al., Published 19 January 2019, Proceedings of the 3rd International Conference on Cryptography
- I still See You! Inferring Fitness Data from Encrypted Traffic of Wearables, Andrei Kazlouski et al., Published in HEALTHINF 2021

Depth coverage

Surveys to Security/Privacy risks of wearable devices:

- A Survey of Wearable Devices and Challenges, Suranga Seneviratne et al., Published 26 July 2017, IEEE Communications Surveys Tutorials
- A Survey of Privacy Vulnerabilities of Mobile Device Sensors, Paula Delgado-Santos et al., 2021, ACM Computing Surveys (CSUR)

Security Threats/Password Leaks:

- MoLe: Motion Leaks through Smartwatch Sensors, He Wang et al., Published 7 September 2015, Proceedings of the 21st Annual International Conference on Mobile Computing and Networking
- When Good Becomes Evil: Keystroke Inference with Smartwatch, Xiangyu et al., Published 12 October 2015, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security

Privacy threats:

- Privacy implications of accelerometer data: a review of possible inferences, Jacob Leon Kröger et al., Published 19 January 2019, Proceedings of the 3rd International Conference on Cryptography
- I still See You! Inferring Fitness Data from Encrypted Traffic of Wearables, Andrei Kazlouski et al., Published in HEALTHINF 2021

Related work: not mentioned in report but mentioned here

- Understanding Fitness Tracker Users' Security and Privacy Knowledge, Attitudes and Behaviours
- Are Those Steps Worth Your Privacy? Fitness-Tracker Users' Perceptions of Privacy and Utility

Tentative report skeleton

1. Introduction
2. IoT wearable hardware: Smartwatches and Fitness
3. Panorama of Security & Privacy Considerations with IoT wearables
    1. Security risks of Smartwatches and Fitness trackers
    2. Privacy risks of Smartwatches and Fitness trackers
4. Threats to security and privacy from accelerometer data
    1. Breaking passwords
    2. Inferring personal information
5. Conclusion

Tentative schedule

- By 14.05: IoT wearable hardware
- By 21.05: Security threats
- By 28.05: Privacy threats
- By 04.06: Conclusion & Abstract
- By 07.06: Refactoring

Thank You For Listening!