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:** Your smartwatch constantly monitors your body composition (fat, water, muscle mass, and blood oxygen) and activities (temperature, heart rate, and sleep). This data then gets synced to your devices and the company's servers.
- **Data Transfer Between Watch and Phone:** Wi-Fi and Bluetooth security have improved in recent years. However, these connectivity technologies remain vulnerable to data breaches.
- **Location-based threats:** Your watch can use GPS data to create a route map of your outdoor workout or commute.

Security and Privacy Threats

- **Third-party companies:** If this data is stored by multiple other downstream companies, this represents a greater breach risk.
- **Unlocking the smart home:** Certain wearables could be used to control smart home devices.
- **Accelerometer:** Accelerometer data helps your smartwatch track movement for health and fitness features This accelerometer data can also be analyzed to **reveal passwords** and credit card numbers.

Width coverage

Surveys to Security/Privacy risks of wearable devices:

- A Survey of Wearable Devices and Challenges
- A Survey of Privacy Vulnerabilities of Mobile Device Sensors

Security Threats/Password Leaks:

- MoLe: Motion Leaks through Smartwatch Sensors
- When Good Becomes Evil: Keystroke Inference with Smartwatch
- WristSnoop: Smartphone PINs prediction using smartwatch motion sensors

Privacy threats:

- Privacy implications of accelerometer data: a review of possible inferences
- I still See You! Inferring Fitness Data from Encrypted Traffic of Wearables

Depth coverage

Surveys to Security/Privacy risks of wearable devices:

- A Survey of Wearable Devices and Challenges
- A Survey of Privacy Vulnerabilities of Mobile Device Sensors

Security Threats/Password Leaks:

- MoLe: Motion Leaks through Smartwatch Sensors
- When Good Becomes Evil: Keystroke Inference with Smartwatch
- WristSnoop: Smartphone PINs prediction using smartwatch motion sensors

Privacy threats:

- Privacy implications of accelerometer data: a review of possible inferences
- I still See You! Inferring Fitness Data from Encrypted Traffic of Wearables

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. Related work
3. Security threats
4. Privacy threats
5. Conclusion

Tentative schedule

- By 24.11: Related work
- By 01.12: Security threats
- By 07.12: Privacy threats
- By 14.12: Conclusion & Abstract
- By 21.12: Refactoring

Thank You For Listening!