



Smartwatches and Fitness trackers: Cyberphysical Privacy and Security Threats
IoT and Security

Henrik Strangalies Freie Universität Berlin

June 23, 2023

Outline



Motivation

Panorama of Security & Privacy Considerations with IoT wearables Confidentiality Integrity Availability

Threats to security and privacy from accelerometer data

Motivation behind IoT wearables: Smartwatches and Fitness Trackers



- Wearable devices have become increasingly popular due to their convenience and functionality.
- ► Enabling users to perform various tasks such as **making payments**, **monitoring health**, and **receiving messages**.



- Wearable devices have become increasingly popular due to their convenience and functionality.
- Enabling users to perform various tasks such as making payments, monitoring health, and receiving messages.
- Along with these benefits, wearables bring forth security and privacy concerns:
 - Data Collection.
 - ▶ **Data Transfer** between wearable device and phone.
 - Applications of third-party companies.
 - Location-based threats.

Panorama of Security & Privacy Considerations with IoT wearables



A Survey of Wearable Devices and Challenges

Article in IEEE Communications Surveys & Tutorials - July 2017		
DOI: 10.1109/COMST.2017.2731979		
CITATIONS	READS	
529	24,844	



Motivation

Panorama of Security & Privacy Considerations with IoT wearables Confidentiality

Availability

Threats to security and privacy from accelerometer data



Definition

Threats to Confidentiality encompasses those where attackers get unauthorised access to information using techniques such as eavesdropping the wireless channel.

Threats of Confidentiality

- ▶ .



- Eavesdropping is the unauthorized real-time interception of a private communication which can expose user's personal information to an attacker.
- Similarly, the authors of the Open Effect Report from 2016 [?] investigated BLE privacy provision in number of fitness tracking devices such as Fitbit Charge HR, Jawbone UP 2, Garmin Vivosmart, Apple Watch, and Xiaomi Mi Band and came to the conclusion all tested devices, except Apple Watch, use the static device addresses that allowed attackers to track user information such as location, time of fitness activities, and reversing user profile by eavesdropping on these devices' communications.

•

Traffic analysis



Freie Universität Berlin

Infomration Gathering Attacks.

Outline



Motivation

Panorama of Security & Privacy Considerations with IoT wearables

Confidentiality

Integrity

Availability

Threats to security and privacy from accelerometer data

Threats to Integrity



Make Titles Informative.



Make Titles Informative.





Motivation

Panorama of Security & Privacy Considerations with IoT wearables

Confidentiality Integrity

Availability

Threats to security and privacy from accelerometer data

Take Home Messages



- ► The first main message of your talk in one or two lines.
- ► The second main message of your talk in one or two lines.
- Perhaps a third message, but not more than that.

- Outlook
 - Something you haven't solved.
 - Something else you haven't solved.

For Further Reading I





A. Author. Handbook of Everything. Some Press, 1990.



S. Someone.
On this and that.
Journal of This and That, 2(1):50–100, 2000.