Freie Universität Berlin

Smartwatches and Fitness trackers: Cyberphysical Privacy and Security Threats

IoT and Security

Henrik Strangalies
Freie Universität Berlin

June 26, 2023

Outline

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.

Freie Universität Berlin

A Survey of Wearable Devices and Challenges

Article *in* IEEE Communications Surveys & Tutorials · July 2017

DOI: 10.1109/COMST.2017.2731979

Outline

Confidentiality

Definition

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

Eavesdropping

- Eavesdropping is the unauthorized real-time interception of a private communication which can expose user's personal information to an attacker.
- 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

- Traffic analysis attacks in the context of wearables involve monitoring communication patterns between devices.
- Privacy vulnerabilities have been identified in Bluetooth Low Energy (BLE) communication between fitness trackers and smartphones.
- Adversaries can track users by analyzing BLE advertisements and static device addresses.
- User activities can be inferred from the size and number of data packets in BLE traffic, even if the packets are encrypted.
- Unique walking patterns can also be used to identify individuals within a small group, even with random addresses [1].
- It has been shown that the majority of fitness trackers use unchanged BLE addresses during advertising, making it feasible to track them.
- The BLE traffic of the fitness trackers is found to be correlated with the intensity of the user's activity, enabling an eavesdropper to determine the **user's current activity** (walking, sitting, idle, or running) through analysis of the BLE traffic.

Infomration Gathering Attacks.

- Passive monitoring of wearable device transmissions enables adversaries to collect data exchanged between wearables and their hubs.
- This information can be used for information gathering attacks, including breaking key exchanges in Bluetooth Low Energy (BLE) pairing and gathering information about user's other devices.
- Researchers have demonstrated attacks that break BLE legacy pairing, infer keystrokes on smartphone touchpads using smartwatch motion sensors, decode keystrokes on keyboards using smartwatch sensors, and infer a user's personal PIN sequence using wearable devices.
- Adversaries can gain access to smartwatches by installing malicious applications to record sensor activities.
- These attacks leverage sensor data captured by wearables and can be executed by sniffing BLE communications or installing malicious apps on wearables [**?**].

Outline

Threats to Integrity

Definiton

Threats to Integrity includes the cases where attackers alter data or information without authorisation. Threats to Availability are the situations where attackers act to deny services to the entities who are authorised to use them.

¸TODO: Doch lieber nur eine Folie für alle attacken nehmen...

Make Titles Informative.

Make Titles Informative.

Outline

Definiton

Threats to Availability are the situations where attackers act to deny services to the entities who are authorized to use them.

Freie Universität Berlin

Conference Paper | Full-text available

Privacy Implications of Accelerometer Data: A Review of Possible Inferences

January 2019
DOI: 10.1145/3309074.3309076
Conference: ICCSP 2019

Jacob Leon Kröger · Philip Raschke · Towhidur Rahman Bhuiyan

Activity And Behavior Tracking

- Accelerometers are used in step counters to estimate **energy expenditure** and **distance walked**, and in medical studies to assess **sedentary time and physical activity**.
- They enable real-time **body posture** and **activity classification**, including basic activities like running, walking, and sitting, as well as more complex activities like writing, typing, and painting.
- They can also monitor **sleep patterns and behaviors**.
- They can detect **hand gestures, eating and drinking moments, smoking, and even distinguish levels of intoxication**.
- They have been used to detect **carried loads and estimate carried weight**, **measure driving behavior**, **analyze speech activity** and **social interactions**, and **reconstruct speech from recorded vibrations**.

Location Tracking

- Studies have demonstrated that accelerometers in mobile devices can be utilized for **user localization and reconstruction of travel trajectories**, even in the absence of GPS or other localization systems.
- Researchers have achieved **geographically tracking individuals driving a car** solely based on accelerometer readings from their smartphones.
- Another study focused on using smartphone accelerometers to determine the **location of the user within a metropolitan train system**.

User Identification

- Ability to differentiate between and uniquely identify users **based on their body movement patterns**.
- Biometric features such as **gait, hand gestures, and head movements** have been used for user identification with high accuracy.
- Capability distinguish between different speakers accurately by sound vibrations, including human speech, with enough quality to .
- The trajectory of a mobile device can reveal a **user's work and home addresses**.
- When combined with other auxiliary datasets, such as white pages or employment directories, it can potentially expose a user's real identity.
- Calibration errors in accelerometers have been found sufficient to create a device "fingerprint" that can track users across website visits, even when other tracking technologies like cookies are blocked.

Keystroke Logging

- The input that users type into their devices, whether through touchscreens or keyboards, often contains highly sensitive information such as text messages, personal notes, login credentials, and transaction details.
- Researchers have demonstrated to infer tap- and gesture-based inputs, including **PINs and graphical password patterns**.
- Entire sequences of text entered through a phone's touchscreen have been obtained using accelerometer data.

Keystroke Logging

- The input that users type into their devices, whether through touchscreens or keyboards, often contains highly sensitive information such as text messages, personal notes, login credentials, and transaction details.
- Researchers have demonstrated to infer tap- and gesture-based inputs, including **PINs and graphical password patterns**.
- Entire sequences of text entered through a phone's touchscreen have been obtained using accelerometer data.
- Later we will talk about a paper that particularly facing the topic of inferring typed words.

- By analyzing accelerometer data from smartphones, researchers have been able to approximate **users' body weight and height**.
- The amount of physical activity can reveal information about **latent chronic diseases, mobility, cognitive function, and even the risk of mortality**.
- Accelerometer data allows for the derivation of various activity-related variables such as **energy expenditure, activity type, and temporal activity patterns**.
- Sleep duration is anotherimportant factor in population health, and accelerometers in wearable devices have been utilized to evaluate **sleep patterns, fragmentation, and efficiency**.
- Specialized accelerometers have been employed to measure additional health parameters, including **voice health, postural stability, and physiological sound**.

.

Inference of Demographics

- Data from body-worn accelerometers can be used to estimate demographic variables such as **age and gender**.
- Differences in **walking smoothness** between adults and children can be detected through accelerometer readings.
- Notably, accelerometer-based gender recognition can work independently of a person's weight and height.
- Additionally, acoustic vibrations captured through a smartphone accelerometer can be used to classify speakers as male or female with high accuracy.

Mood and Emotion Recognition

- Physical activity, as measured by body-worn accelerometers, has been linked to human emotions and depressive moods.
- Researchers have used accelerometer data from smart wristbands to recognize emotional states, such as **happiness, neutrality, and anger**, with fair accuracy.
- Accelerometers in smartphones have been employed to detect **stress levels and arousal in users**.
- Additionally, there is a positive association between accelerometer-derived s**peech activity and mood changes**.

Inference of Personality Traits

- Methods have been developed to infer **preferences and personality traits** based on body gestures and motion patterns captured by accelerometers.
- Wearable accelerometers were used to estimate the **motivations, interests, and group affiliations** of study participants during social interactions, relying on their movements, body postures, and gesturing patterns.
- Studies have shown that **conscientiousness, neuroticism, openness, and extraversion** are associated with different levels of physical activity.
- Moreover, it has been discovered that neuroticism and the functioning of the behavioral inhibition system were related to physical activity measures derived from accelerometer data in female college students.

Conference Paper

MoLe: Motion Leaks through Smartwatch Sensors

September 2015
DOI: 10.1145/2789168.2790121
Conference: the 21st Annual International Conference

He Wang · Ted Tsung-Te Lai · Romit Roy Choudhury

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.