



Smartwatches and Fitness trackers: Cyberphysical Privacy and Security Threats

IoT & Security

Henrik Strangalies
Freie Universität Berlin

July 4, 2023

Motivation

Panorama of security and privacy considerations with IoT wearables

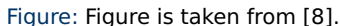
- Threats to Confidentiality

- Threats to Integrity

- Threats to Availability

Threats to security and privacy from accelerometer data

Inferring typed words on keyboard using accelerometer and gyroscope data



- Computer Science, IoT & Security, Privacy & Security Threats of IoT Wearables ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡|≡ ↺ 🔍 ↻ 3

A Survey of Wearable Devices and Challenges

Article in IEEE Communications Surveys & Tutorials · July 2017

DOI: 10.1109/COMST.2017.2731979

CITATIONS

529

READS

24,844

Motivation

Panorama of security and privacy considerations with IoT wearables

Threats to Confidentiality

Threats to Integrity

Threats to Availability

Threats to security and privacy from accelerometer data

Inferring typed words on keyboard using accelerometer and gyroscope data

Definition

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

- ▶ Most existing wearable devices use Bluetooth Low Energy (BLE) as the major means of communication.
- ▶ BLE equipped wearable devices have been reported to be vulnerable to attacks that impact the confidentiality such as eavesdropping and traffic analysis.
- ▶ **Eavesdropping** is the unauthorized real-time interception of a private communication which can expose user's personal information to an attacker.
- ▶ **Traffic analysis attacks** in the context of wearables involve monitoring communication patterns between devices.
- ▶ **Information gathering attacks** include passive monitoring of wearable device transmissions enables adversaries to collect data exchanged between wearables and their hubs.

Motivation

Panorama of security and privacy considerations with IoT wearables

Threats to Confidentiality

Threats to Integrity

Threats to Availability

Threats to security and privacy from accelerometer data

Inferring typed words on keyboard using accelerometer and gyroscope data

Definiton

Threats to Integrity includes the cases where attackers alter data or information without authorisation.

- ▶ **Modification attacks:** Adversaries can intercept and modify data exchanged between wearable devices, including changing packet content and timestamps.
- ▶ In **replay attacks**, adversaries capture valid data packets uploaded by a wearable device and replay them for malicious purposes such as impersonation or data corruption.
- ▶ **Masquerade attacks** involve impersonating an authenticated device to steal data or inject fake information.

Motivation

Panorama of security and privacy considerations with IoT wearables

Threats to Confidentiality

Threats to Integrity

Threats to Availability

Threats to security and privacy from accelerometer data

Inferring typed words on keyboard using accelerometer and gyroscope data

Definiton

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

- ▶ For instance, the FitBit Charge tracker can be targeted with DoS attacks to **prevent legitimate device syncing or pairing** with mobile phones.
- ▶ Attack tools like Fitbite and GarMax have been used to inject fake data, **exceeding the storage capacity of trackers**, thereby preventing them from recording valid user data.
- ▶ These attacks can **drain the battery** by continuously querying the nearby trackers.

Full-text available

Privacy Implications of Accelerometer Data: A Review of Possible Inferences

January 2019

DOI: [10.1145/3309074.3309076](https://doi.org/10.1145/3309074.3309076)

Conference: ICCSP 2019

 Jacob Leon Kröger · Philip Raschke · Towhidur Rahman Bhuiyan

Research Interest Score _____ 30.1

Citations 46

Recommendations 2

Reads ⓘ 3.697

Learn about stats on ResearchGate

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**.
- ▶ Researchers were able to distinguish **sober walk** from **intoxicated walk** and to estimate **blood alcohol content** as well as the **number of drinks consumed**.
- ▶ 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**.

- ▶ 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**.

- ▶ 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 to distinguish between different speakers accurately by sound vibrations, including human speech.
- ▶ The trajectory of a mobile device can reveal a **user's work and home addresses**.
- ▶ Calibration errors in accelerometers have been found sufficient to **uniquely identify their encapsulating device** so that users can be tracked across website visits, even when private browsing is activated or when other tracking technologies like cookies are blocked.

- ▶ 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.

- ▶ 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**.
- ▶ Sleep duration is another important 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**.

- ▶ 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.

- ▶ 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 **speech activity and mood changes**.

- Computer Science, IoT & Security, Privacy & Security Threats of IoT Wearables ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡|≡ ↺ 🔍 ↻ 22

Conference Paper

MoLe: Motion Leaks through Smartwatch Sensors

September 2015

DOI: [10.1145/2789168.2790121](https://doi.org/10.1145/2789168.2790121)

Conference: the 21st Annual International Conference

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

Research Interest Score 116.3

Citations 233

Recommendations 0

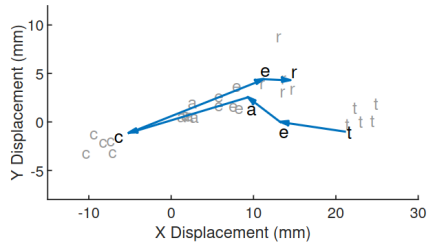
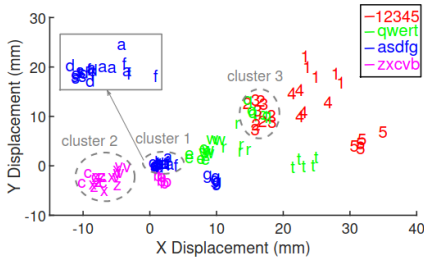
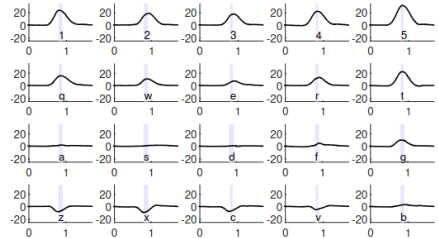
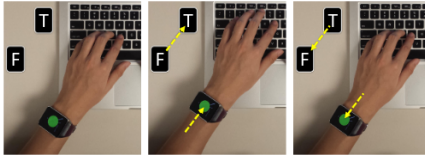
Reads ⓘ 208

[Learn about stats on ResearchGate](#)

- ▶ Imagine a user typing on a laptop keyboard while wearing a smart watch.
- ▶ This paper asks whether motion sensors from the watch can leak information about what the user is typing.
- ▶ Thereby compromising the privacy of a **user's emails, search queries, personal notes and other documents typed** on the keyboard.
- ▶ The activity tracker malware can obtain the user's permission and easily launch a side channel attack.

- ▶ Smartwatch is worn on the left hand.
- ▶ The absence of data from the right hand is a unique constraint, and so it needs to infer which finger executed the key-press.
- ▶ For a given position of the wrist watch, it is not obvious which one of the 3 or 4 different keys could have been pressed, which could be further interspersed by unknown number of keys pressed by the right hand.
- ▶ Users write different with dexterity, e.g. some use their little finger far less efficiently while others use specific fingers when it comes to digits or corner keys.

Procedure of the data collection



Figures are taken from [1].

Attacker Labeled Typed Data

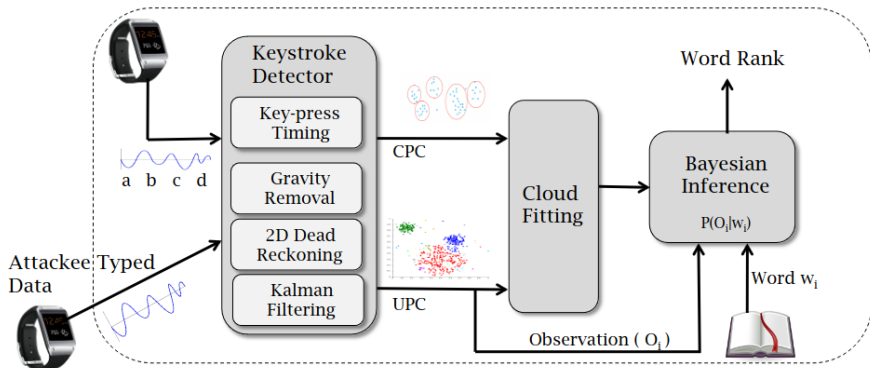
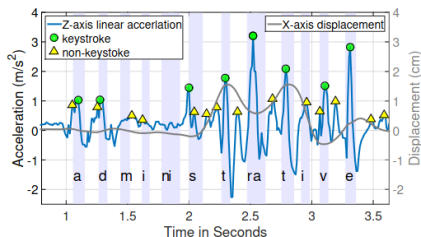
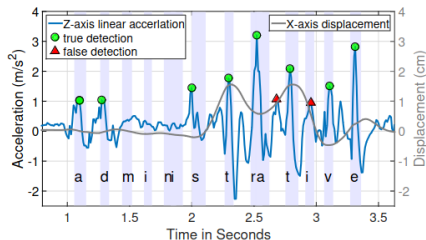


Figure: Figure is taken from [1].

This paper defines the following conditions for their experiment:

- ▶ Volunteers type **one word at a time** (as opposed to free-flowing sentences).
- ▶ **Only valid English words** are allowed: Passwords that contain interspersed digits, or non-English character-sequences, are not decodable as of now.
- ▶ The same Samsung smart watch model was used for both the attacker and the user.
- ▶ They assumed the user is seasoned in typing in that he/she roughly uses the appropriate fingers – novice typists who do not abide by basic typing rules may not be subject to the proposed attacks.



Figures are taken from [1].

Key-press Location Estimation

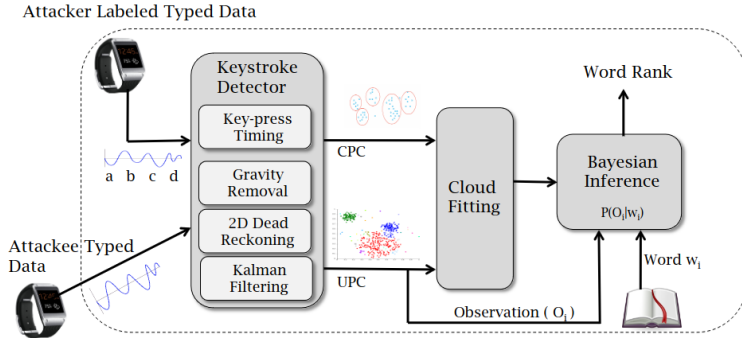


Figure: Figure is taken from [1].

- Initially, Android API's linear acceleration data was used but it was unsatisfactory and they developed a tailored tracking approach by themselves.

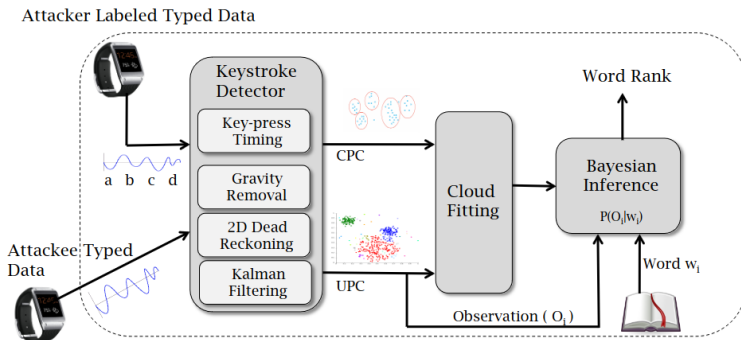
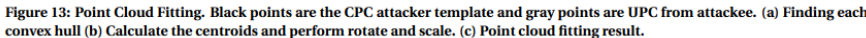


Figure: Figure is taken from [1].

- ▶ MoLe generates an unlabeled point cloud (UPC) based on the estimated displacements for each key pressed by the attacker.
- ▶ To assign approximate labels to the points in the UPC, MoLe fits the attacker's character point cloud (CPC) to the UPC. The fitting process involves computing convex hulls for both the CPC and the UPC.



Computer Science, IoT & Security, Privacy & Security Threats of IoT Wearables ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡|≡ ↺ 🔍 ↻ 32

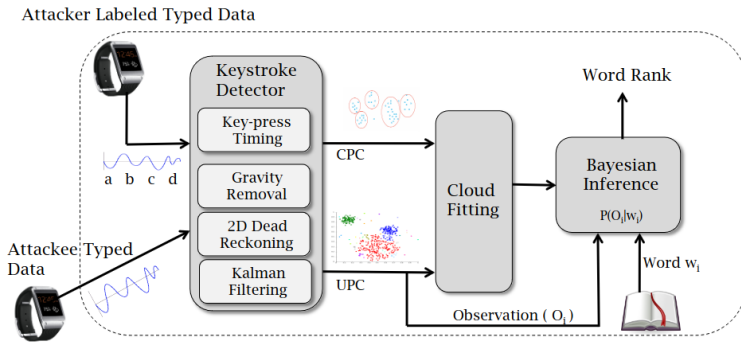


Figure: Figure is taken from [1].

- ▶ Even if the keystroke detection and point cloud fitting are perfect, MoLe still does not know the characters typed by the right hand.
- ▶ MoLe aims to infer the characters typed by the right hand, filling in the missing information.

Bayesian Inference - Refinements

- ▶ One approach is to consider **the number of detected keystrokes as observations** to match the word. The number of keys typed by the left hand is used to evaluate the likelihood of each word.
- ▶ Additionally, for cases where **two consecutive characters** are detected **as a single keystroke** due to close succession, treating them as one key-press can be appropriate.
- ▶ Given that the CPC has been fitted to the user's UPC, it is now possible to better predict the word by **taking displacement into consideration**.
- ▶ Typing a word consists of sequential movements and the current displacement is indeed influenced by the location of the **previous character**.
- ▶ The encoding of information about missing keys can be inferred from the timing of left-hand key presses, and the objective is to determine the probability of having N right-hand characters between consecutive keystrokes based on the **detected time interval**.

- ▶ Accelerometer and gyroscope readings were recorded at 200Hz on the Galaxy Gear Live smartwatch.
- ▶ Eight volunteers were recruited familiar with English typing, each typed 300 English words randomly selected from the 5000 most frequently used words.
- ▶ A word appeared one at a time on the laptop screen, and the subjects were instructed to type the same word in a text box on the screen.
- ▶ If any characters were mistyped, the data was discarded, and the subject was asked to re-enter the word.
- ▶ Subjects were instructed to initialize their hand position on the "F" and "J" keys between each word recording.
- ▶ The laptop recorded the timing of the keystrokes, which served as the ground truth.

- ▶ To collect training data, two of the authors acted as attackers and followed the **same procedure**, but with the top 500 longest words in the dictionary.
- ▶ For full ground truth recording, an Android Samsung Galaxy S4 phone was mounted on top of the keyboard, and the front camera was used to capture video of hand movement.
- ▶ The camera calibration toolbox in MATLAB was used to calibrate the camera pixel and measure the watch distance and location from each frame.

Cumulative Distribution Function of Rank

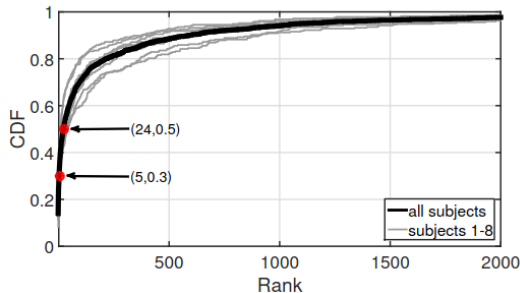


Figure: Figure is taken from [1].

- ▶ Figure illustrates the cumulative distribution function (CDF) of rank.
- ▶ The results indicate that the median rank of a word is 24, i.e. there is a 50% chance that MoLe can narrow down the typed word to 24 possibilities.
- ▶ At the 30th percentile, the rank is 5, indicating a 30% chance of narrowing down the possibilities to **just 5 words**.

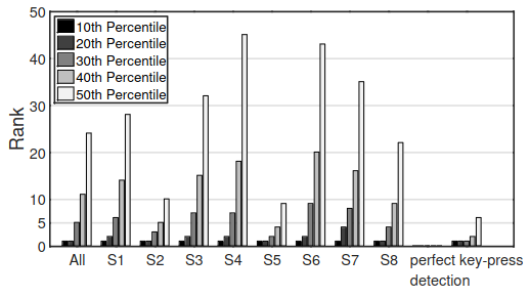


Figure: Figure is taken from [1].

- ▶ Figure displays the ranks of typed words for each test subject.
- ▶ The authors state that the system performance is close between two keyboards, even though the attackers used the laptop keyboard for training the system.

Example

Rank	W_1	W_2	W_3	W_4	W_5	W_6	W_7	W_8
1.	motor	pistol	profound	technology	angel	those	that	disappear
2.	monitor	list	journalism	remaining	spray	today	tight	discourse
3.	them	but	originally	telephone	super	third	tightly	secondary
4.	the	lost	original	meanwhile	fire	through	thirty	adviser
5.	then	most	profile	headline	shore	towel	truth	discover

Figure: Table is taken from [1].

- ▶ Table displays MoLe's end-to-end prediction results for each word in an actual sentence entered by subject S5.
- ▶ The table lists the Top-5 guesses for each word, with the most likely guess at the top.
- ▶ The words in each column exhibit similarity in their character sequences.

Example

Rank	W_1	W_2	W_3	W_4	W_5	W_6	W_7	W_8
1.	motor	pistol	profound	technology	angel	those	that	disappear
2.	monitor	list	journalism	remaining	spray	today	tight	discourse
3.	them	but	originally	telephone	super	third	tightly	secondary
4.	the	lost	original	meanwhile	fire	through	thirty	adviser
5.	then	most	profile	headline	shore	towel	truth	discover

Figure: Table is taken from [1].

- ▶ Table displays MoLe's end-to-end prediction results for each word in an actual sentence entered by subject S5.
- ▶ The table lists the Top-5 guesses for each word, with the most likely guess at the top.
- ▶ The words in each column exhibit similarity in their character sequences.
- ▶ Reconstructed sentence:

The most profound technologies are those that disappear.





- ▶ MoLe is not able to infer non-valid English words, such as passwords.
- ▶ There is no scalability across different watch models.
- ▶ Training and test data contain no mistake such as mistyping and pressing delete key.
- ▶ Subjects were instructed to follow the typing guideline such as returning to "F"-Key.
- ▶ It is capable to parse sentences due to difficulties in detecting the "space bar".
- ▶ Despite the authors' assertion that the disparity between the two keyboards is minimal, their evaluation was limited to testing only two selected models.
- ▶ However, the authors state that although no tests were made with other wearable devices such as Fitbits, they believe with some customization, the attacks can be launched on those platforms as well.

- ▶ MoLe is not able to infer non-valid English words, such as passwords.
- ▶ There is no scalability across different watch models.
- ▶ Training and test data contain no mistake such as mistyping and pressing delete key.
- ▶ Subjects were instructed to follow the typing guideline such as returning to "F"-Key.
- ▶ It is capable to parse sentences due to difficulties in detecting the "space bar".
- ▶ Despite the authors' assertion that the disparity between the two keyboards is minimal, their evaluation was limited to testing only two selected models.
- ▶ However, the authors state that although no tests were made with other wearable devices such as Fitbits, they believe with some customization, the attacks can be launched on those platforms as well.

⇒ **MoLe is not yet a real-world attack.**

- ▶ Wearable devices have gained significant popularity due to their convenience and versatility, enabling users to engage in various activities such as making payments, monitoring health, and receiving notifications.
- ▶ The presentation introduced briefly threats to confidentiality, integrity and availability.
- ▶ The presentation summarized potential threats posed by accelerometer and gyroscope data collected by wearables.
- ▶ The presentation delved into the findings of a research paper that examines the vulnerabilities associated with analyzing motion sensor data to decipher keyboard inputs.

For Further Reading I

-  Seneviratne, Suranga et al. "A Survey of Wearable Devices and Challenges." IEEE Communications Surveys & Tutorials 19 (2017): 2573-2620.
-  Delgado-Santos, Paula et al. "A Survey of Privacy Vulnerabilities of Mobile Device Sensors." ACM Computing Surveys (CSUR) 54 (2022): 1 - 30.
-  Wang, He et al. "MoLe: Motion Leaks through Smartwatch Sensors." Proceedings of the 21st Annual International Conference on Mobile Computing and Networking (2015): n. pag.
-  Liu, Xiangyu et al. "When Good Becomes Evil: Keystroke Inference with Smartwatch." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (2015): n. pag.
-  Kröger, Jacob Leon et al. "Privacy implications of accelerometer data: a review of possible inferences." Proceedings of the 3rd International Conference on Cryptography, Security and Privacy (2019): n. pag.

- Computer Science, IoT & Security, Privacy & Security Threats of IoT Wearables ◀ ◻ ▶ ◀ ◻ ▶ ◀ ≡ ▶ ◀ ≡ ▶ ≡|≡ ↺ 🔍 ↻ 43