Freie Universität Berlin

# Smartwatches and Fitness trackers: Cyberphysical Privacy and Security Threats

IoT and Security

Henrik Strangalies
Freie Universität Berlin

July 2, 2023

# Outline

## 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

# Motivation behind IoT wearables: Smartwatches and Fitness Trackers


Figure: Figure is taken from [8].

- 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**.


Figure: Figure is taken from [8].

- 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

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

# 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 [7] 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.
- This report 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**.
- Adversaries can track users by analyzing Bluetooth Low Energy (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.
  - 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.

# Information 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.

# Outline

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

# Threats to Integrity

## 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**.
- Vulnerabilities have been found in Bluetooth LE pairing, fitness data storage, and transmission in popular trackers such as **FitBit and Garmin**.
- Timestamp integrity in healthcare devices has also been compromised, allowing attackers to **tamper with medical data**.
- The **lack of HTTPS transmission** in certain applications exposes sensitive fitness data to unauthorized parties, enabling data falsification.

# Replay Attacks

- 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.
- An example for a replay attack was demonstrated in a commercially available insulin delivery system:
  Here, attackers were able to determine the packet format and learn the **device type, its PIN, the therapy or glucose level, and medical condition of the patient** as they are transmitted in plaintext by eavesdropping on the communication between devices.

# Masquerade Attacks

- Masquerade attacks involve **impersonating an authenticated device to steal data or inject fake information**.
- Examples include collecting bonding information from medical devices through malicious apps and controlling insulin pumps by knowing the device’s PIN.
- **These attacks exploit the lack of authentication and encryption in wearable systems.**
- While threats to integrity are less common than those to confidentiality, addressing data confidentiality vulnerabilities will also protect data integrity.

# Data Breaches

- The massive data collection provides users with **plenty features** to track theirs health, but can lead to **data breaches**.
- Smartwatches and fitness trackers can monitor physiological parameters like distance walked or run using motion sensors and GPS, heart rate, ECG, stress levels, sleep quality, and more.
- Heart-related metrics and polysomnographic parameter can be measured due to optical sensors are commonly integrated into smartphones and smartwatches to **detect variations in blood volume** within the arteries beneath the skin.
- It has been shown that the identification of various activities such as **stationary behavior, walking, running, bicycling, stair climbing, descent, and driving** was achieved solely through the utilization of accelerometer data.
- Information pertaining to sleep, including **sleep posture, habits hand position during sleep** has been successfully extracted using accelerometer, gyroscope, and orientation data from a smartwatch.

# Outline

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

# Threats to Availability

**Definiton**

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

# Threats to Availability

- Denial of Service (DoS) attacks are a common type of attack against **availability in wearable devices**.
- They aim to disrupt communication between wearables and their base or overwhelm the device’s storage capacity with useless information.
- 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 batter**y by continuously querying the nearby trackers.

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 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**.
- 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 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**.

.

# 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 **speech 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.

# Inferring Typed Words

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

# Motivation

- The paper highlights the significant ramifications of such data leakage, as smartwatches **can be camouflaged as activity trackers**.
- Thereby compromising the privacy of a **user's emails, search queries, and other documents typed** on the keyboard.
- The activity tracker malware can obtain the user's permission and easily launch a side channel attack.

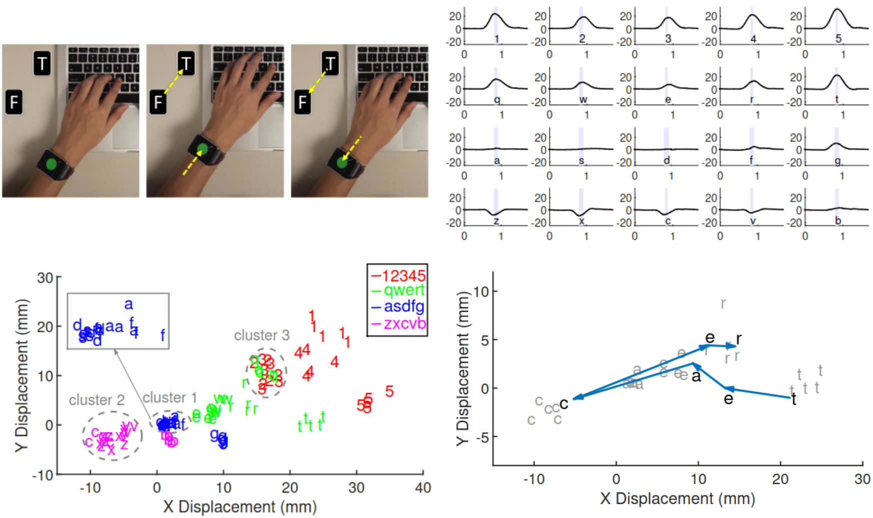
# Assumptions and Constraints

- 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.

# Data Collection

- **Training data:** Two authors put on Samsung Gear Live smart watches and typed 500 words recording the accerlerometer and gyroscope data.
- The training data is processed through a sequence of steps, including key-press detection, hand-motion tracking, character point cloud computation, and Bayesian modeling and inference.
- The **test data** was collect by 8 different volunteers who were asked to type 300 different English words from a dictionary.
- The smart-watch sensor data from the volunteers was used to create a short-lists *K* words, ranked in the decreasing order of probability (i.e., the first ranked word is considered the most probable guess.

# Collection Procedure




Figures are taken from [1].

# MoLe: Overview

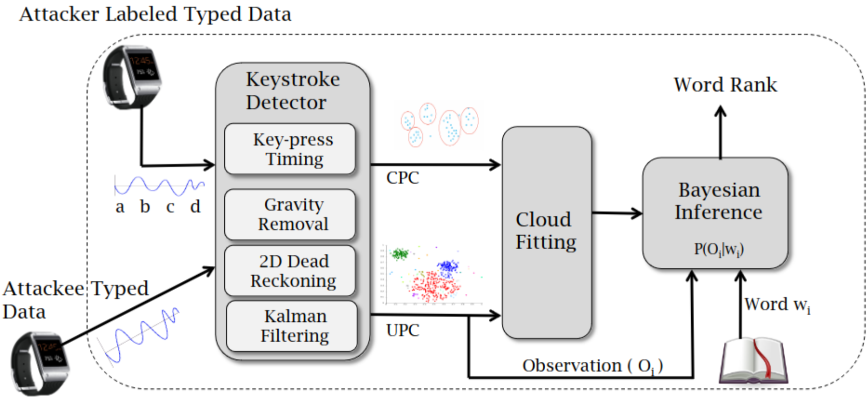


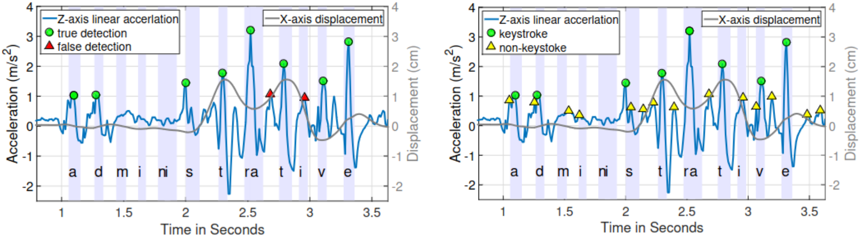

Figure: Figure is taken from [1].

# Constraints

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.

# Keystroke Detector




Figures are taken from [1].

# Key-press Location Estimation

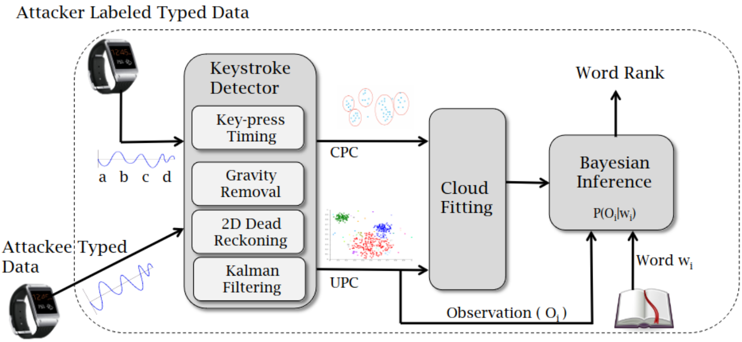



Figure: Figure is taken from [1].

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

# Point Cloud Fitting

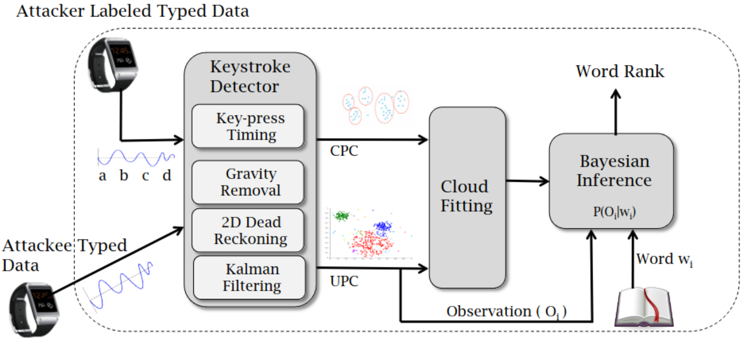



Figure: Figure is taken from [1].

- 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.

## Point Cloud Fitting

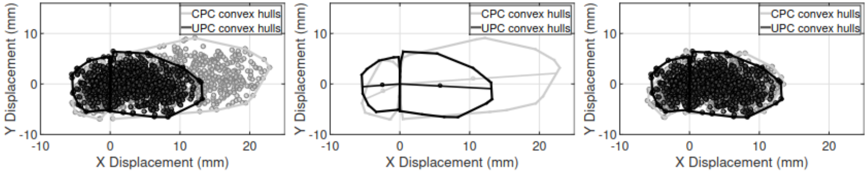



**Figure 13: Point Cloud Fitting. Black points are the CPC attacker template and gray points are UPC from attackee. (a) Finding each convex hull (b) Calculate the centroids and perform rotate and scale. (c) Point cloud fitting result.**

Figure is taken from [3].

# Bayesian Inference

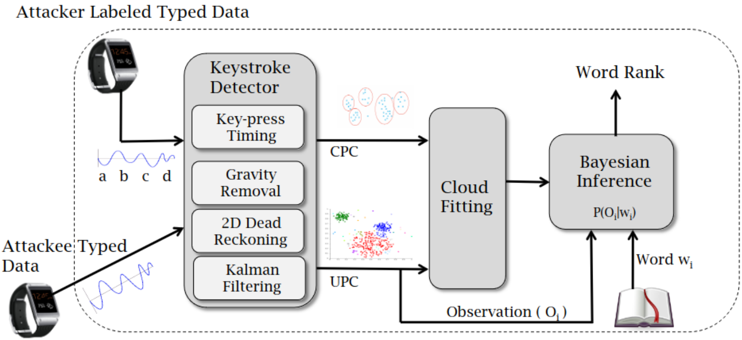



Figure: Figure is taken from [1].

- 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**.

# Setup Test Data

- 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.

# Setup Training Data

- 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

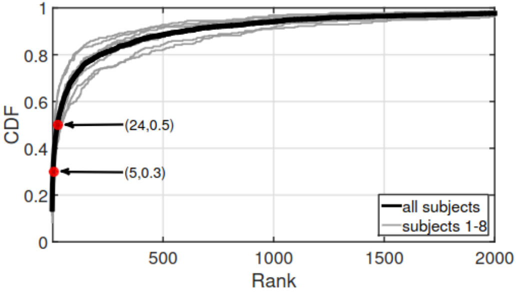



Figure: Figure is taken from [1].

- 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**.

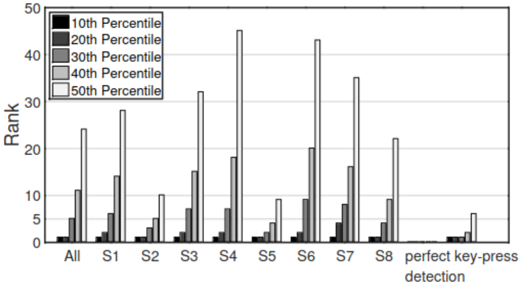



Figure: Figure is taken from [1].

- 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.**

# Limitations

- 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.

# Limitations

- 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.

$\Rightarrow$ **MoLe is not yet a real-world attack.**

# 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.

# 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.

# For Further Reading II


- R. Goyal, N. Dragoni, and A. Spognardi, "Mind the tracker You wear: A security analysis of wearable health trackers," in Proceedings of the 31st Annual ACM Symposium on Applied Computing, ser. SAC '16. New York, NY, USA: ACM, 2016, pp. 131–136.
- https://openeffect.ca/reports/Every_Step_You_Fake.pdf, 2016.
- https://cdn.test.de/file/image/87/08/0404382e-ad12-4c12-b8e8-906f8e2d37c7-web/6003370_smartwatches-t202306;a3-2.jpg