WACA: Wearable-Assisted Continuous Authentication

Abbas Acar, Hidayet Aksu, Kemal Akkaya, and A. Selcuk Uluagac

Florida International University

Electrical and Computer Engineering Department

Cyber-Physical Systems Security Lab (CSL)

{aacar001, haksu, kakkaya, suluagac}@fiu.edu

Abstract

One-time login process in conventional authentication systems does not guarantee that the identified user is the actual user throughout the session. However, it is necessary to re-verify the user identity periodically throughout a login session, which is lacking in existing one-time login systems. In this paper, we introduce a usable and reliable wearable-Assisted Continuous Authentication(WACA), which relies on the sensor-based keystroke dynamics and the authentication data is acquired through the built-in sensors of a wearable (e.g., smartwatch) while the user is typing. The acquired data is periodically and transparently compared with the registered profile of the initially logged-in user with one-way classifiers. With this, WACA continuously ensures that the current user is the user who logged-in initially. We implemented the WACA framework and evaluated its performance on real devices with real users. The empirical evaluation of WACA reveals that WACA is feasible and its error rate is as low as 1% with 30 seconds of processing time and2−3%for 20 seconds. The computational overhead is minimal. Furthermore, WACA is capable of identifying insider threats with very high accuracy (99.2%).

Password is not enough

- Leaving your computer **unlocked** is a huge security risk.
- Users **share** their passwords with co-workers and family members.
- **Insiders** have already the passwords.

Even 2FA is not enough

- In 2FA or MFA, there is only **single check-point**
  - After passing it, anyone can use.
- Even if it is an **insider** who has been authorized once, a forever access is provided in most cases not to interrupt the current user.

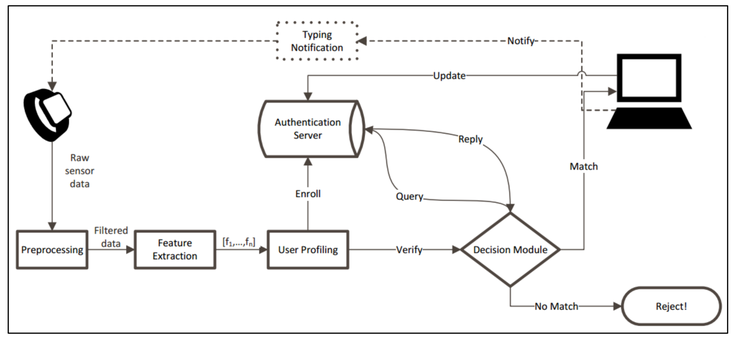
Continuous Authentication (CA) solves these issues, but..

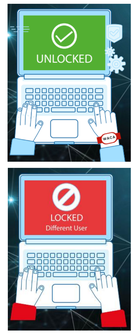
- CA periodically checks the user's identity during the entire session.
- But, they are either not reliable or not usable.
- Not reliable for CA:
  - Time-out
  - Proximity
  - Traditional Keystroke Dynamics
- Not usable for CA:
  - Fingerprint
  - Face
  - Eye movement

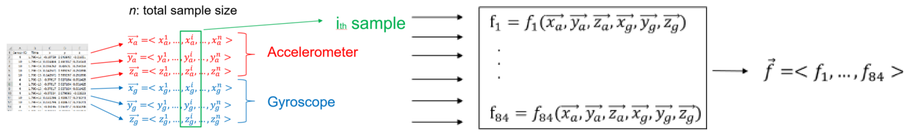
We can use "wearables"

- By 2020, there will be 411 million wearable [1].
- Advance built-in sensors (e.g., accelerometer, GPS, thermometer, heart rate monitoring, etc.).
- Advanced networking capability (e.g., Bluetooth and Wi-Fi).

Overall Architecture of WACA





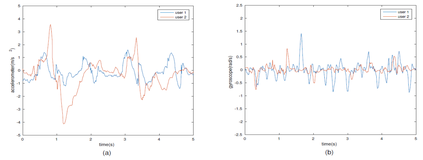


- Aim: Using the ubiquitous nature of wearables for the usability of continuous authentication.
- Key observation: Each person's wrist movements & actions are completely unique while typing.
- WACA:
  - Complementary to the "first factor"
  - Collects data through smartwatch's motion sensors (i.e., accelerometer and gyroscope)
  - Extracts keystroke dynamics from raw sensor data
  - The feature vector (i.e., user profile) is created to profile the user
  - Decision Module:
    - ✓ Authentication using Distance Measure
    - ✓ Identification using Machine Learning Algorithms

Observations

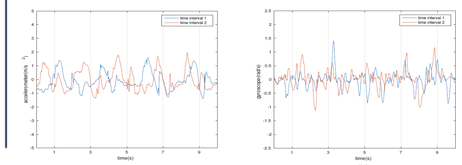
1. First Observation:

- Two different users' sensor data while typing the same text with (a) accelerometer, (b) gyroscope:

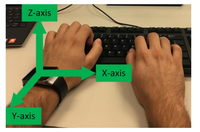


2. Second Observation:

- The same user's sensor data over two different time intervals with (a) accelerometer, (b) gyroscope:



Experimental Setup



- We collected data from **34 participants**
- LG G Watch R and Samsung Gear Live
- Android Wear app to collect sensor data
- Data is collected via **6-axis motion** sensor (3-axis acc + 3-axis gyro)
- Qwerty keyboard
- Task-1: The participants were asked to type a **randomly selected** text
- Task-2: The participants were asked to type the **same** text

Authentication Results

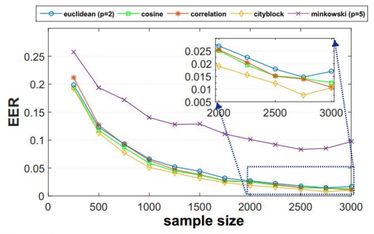


Fig. 7: Average EER according to different sample sizes using different distance metrics while users are performing Typing Task-1.

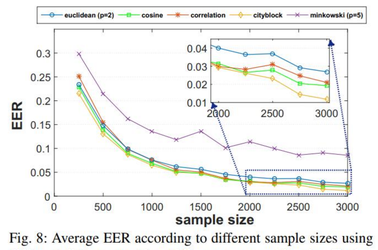


Fig. 8: Average EER according to different sample sizes using different distance metrics while users are performing Typing Task-2.

Identification Results

TABLE III: Scenerio 1: The same text is used for both training and testing using the Multilayer Perceptron algorithm.

The accuracy of insider threat identification (%)

Sample size	Training Set 1	2	3	4	5
1500	77.8	**93.7**	**97.2**	**98.4**	**99.2**
1000	62.8	87.6	**93.8**	**95.3**	**97.1**
500	37.5	63.7	75.9	83.1	89.6
250	28.5	43	53.1	61.8	62.1

TABLE IV: Scenerio 2: All users are trained with the same text and tested with random texts using the Multilayer Perceptron algorithm.

The accuracy of insider threat identification (%)

Sample size	Training Set 1	2	3	4	5
1500	55.8	80.1	88.7	89.8	**91.8**
1000	51.7	82.7	83.2	86.1	86.8
500	29.9	51.3	66.7	73.8	76.5
250	22.1	33.6	41.9	49.8	54.1

References & Acknowledgements

1. **Abbas Acar**, Hidayet Aksu, Kemal Akkaya, and A. Selcuk Uluagac. WACA: Wearable-Assisted Continuous Authentication. In 39th IEEE Symposium on Security and Privacy Workshop, 2018. (to appear)
2. P. Lamkin. Wearable tech market to be worth $34 billion by 2020 @ONLINE, Feb. 2016, http://www.forbes.com/sites/paullamkin/2016/02/17/wearable-tech-market-to-be-worth-34-billion-by-2020/#f3e57cd3fe38
3. S. Mare, A. M. Markham, C. Cornelius, R. Peterson, and D. Kotz. Zebra: zero-effort bilateral recurring authentication. In *Security and Privacy (SP), 2014 IEEE Symposium on*, pages 705(720. IEEE, 2014

This work was partly supported by NSF-CAREER-CNS-1453647 and NSF-CNS-1718116.