HR-Auth: Heart Rate Data Authentication using Consumer Wearables

Alfredo J. Perez
Columbus State University
perez_alfredo@columbusstate.edu

Miguel A. Labrador
University of South Florida
mlabrador@usf.edu

Kevin G. Rivera-Morales
Universidad del Turabo
krivera382@email.suagm.edu

Idalides Vergara-Laurens
Universidad del Turabo
ivergara@suagm.edu

ABSTRACT

We study the authentication of the heart rate (HR) signal and we present HR-Auth, an algorithm to authenticate HR data using two independent wearable sensors. We describe and evaluate the proposed algorithm.

CCS CONCEPTS

• **Security and privacy → Authentication**; • **Networks → Sensor networks**; • **Human-centered computing → Ubiquitous and mobile devices**; • **Applied computing → Consumer health**;

KEYWORDS

Security, authentication, mHealth, heart rate, Internet of Things, wearables, smart health, mobile sensing, Android Wear

ACM Reference Format:
Alfredo J. Perez, Kevin G. Rivera-Morales, Miguel A. Labrador, and Idalides Vergara-Laurens. 2018. HR-Auth: Heart Rate Data Authentication using Consumer Wearables. In *MOBILESoft '18: MOBILESoft '18: 5th IEEE/ACM International Conference on Mobile Software Engineering and Systems , May 27–28, 2018, Gothenburg, Sweden.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3197231.3197254

1 INTRODUCTION

The usage of consumer wearables in mHealth applications may lead to life-threatening consequences when intrusive actions in the human body are performed based on unreliable and faulty sensor data collected through them [3]. Even though solutions to authenticate mHealth sensor data exist as methods based on encryption to authenticate that the data were generated by the sensors [2][4][5], and methods that use active probing to ensure that the analog data have not been spoofed [1], these solutions cannot authenticate (verify) that the values reported in the digital signal correspond to the actual analog signal of the monitored process.

MOBILESoft '18, May 27–28, 2018, Gothenburg, Sweden

ACM ISBN 978-1-4503-5712-8/18/05…$15.00
https://doi.org/10.1145/3197231.3197254

In this work, we describe and evaluate HR-Auth, a method to authenticate heart rate (HR) data using consumer wearables. Our contributions are as follows: (1) our method authenticates HR data without modifying the firmware of the sensors; (2) the method does not require sensor synchronization; (3) our method is lightweight and can be implemented in wearables, smartwatches and mobile phones.

2 THE HR-AUTH ALGORITHM

We make use of the following definitions to describe the algorithm:

Definition 2.1 (Heartbeat). We define a heartbeat as the ordered pair $H = (b, t)$ where $b \in [0, 220]$ and $t \in \mathbb{R}_{>0}$. The value b represents the value of the pulse in bpm (beats per minute), and the value t represents the data value's timestamp in milliseconds.

Definition 2.2 (Validity of Heartbeats). Given any two heartbeats $H_x = (b_x, t_x)$ and $H_y = (b_y, t_y)$ the validity of the heartbeats, denoted by $V(H_x, H_y, \delta)$ is defined as follows:

$$V(H_x, H_y, \delta) = \begin{cases} true & abs(t_x - t_y) \leq 1000 \wedge abs(b_x - b_y) \leq \delta \\ false & otherwise \end{cases}$$

In the definition 2.2, $abs(.)$ denotes the absolute value of a real number. The HR-Auth method (described in algorithm 1) receives the HR data from two independent sensors (first two parameters), the validation threshold δ, a counter variable to track the number of consecutive times that the measurements fail the validation test (*sCount*), and a counter variable to track the number of times the validation test fails throughout the data collection (*dCount*).

3 EVALUATION

We implemented the HR-Auth algorithm for Android Wear 2.0 and we used the Zephyr Bioharness 3 and the Polar M600 smartwatch as shown in figure 1. The Bioharness is a chest wearable that makes use of electrocardiography (ECG) to measure HR and the Polar M600 uses a wrist photoplethysmography (PPG) HR sensor. We chose the value $\delta = 7$ in HR-Auth after collecting a total of 600 data points from a single subject wearing both sensors while sitting, and calculating the average (4.1 bpm) and standard deviation (3.20 bpm) from the collected points. We implemented two smartwatch app versions to test HR-Auth:

Algorithm 1: The HR-Auth Algorithm

Input: $H_{first\_sensor}, H_{second\_sensor}, \delta, sCount, dCount$
Result: $H_{first\_sensor}, H_{second\_sensor}$ are either "authentic" or "corrupted"

```
begin
    if V(H_first_sensor, H_second_sensor, δ) == true then
        Mark H_first_sensor, H_second_sensor heartbeats as "authentic"
        Decrease sCount by 1 if greater than 0
    else
        Mark H_first_sensor, H_second_sensor as "corrupted"
        if abs(H_first_sensor − H_second_sensor) > δ then
            Increase sCount and dCount by 1
        end
        if sCount = MAX_SCOUNT ∨ dCount = MAX_DCOUNT then
            Review all collected data
            Stop data collection
        end
    end
end
```

Figure 1: Hardware architecture for HR-Auth.

- **Version 1:** In this version, HR-Auth is called only when an HR message is received from the Bioharness chest sensor. This can happen at most one time per second since the Bioharness broadcasts HR messages at 1Hz.
- **Version 2:** In this version, HR-Auth is called every time an HR message is received from the Bioharness, or the PPG sensor in the smartwatch generates an event. In this case, HR-Auth may be invoked at a higher frequency than 1Hz since the PPG sensor can generate more than one event (i.e., PPG sensor reading) per second.

We performed two set of experiments: (Experiment 1) 10 tests were carried out with two subjects, each wearing a different sensor to simulate a faulty (or hacked) sensor; (Experiment 2) 10 tests in which a subject wore both sensors. We collected 30 pairs of HR measurements for HR-Auth to mark/classify them as *authentic* or *corrupted* per test. We setup the constant values MAX_SCOUNT and MAX_DCOUNT to be a high value to collect the 30 pairs of data points. The results of the experiments are shown in figure 2.

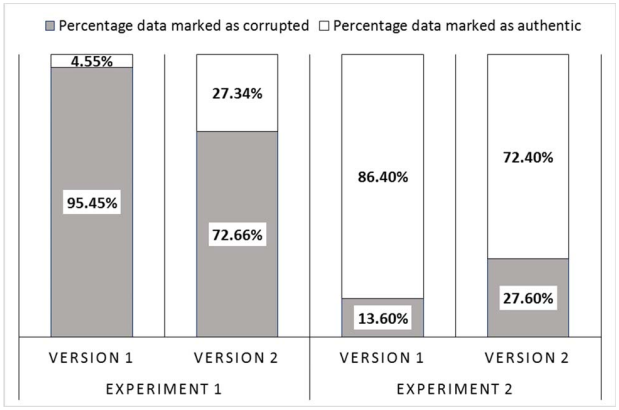

Figure 2: HR-Auth experimental results.

In Experiment 1 we observed that even though HR-Auth was invoked faster in version 2 (438 ms on average after the first sensor reading was performed, against 868.9 ms in version 1), the overall performance in the detection of corrupted data was worse (72.66% in version 2) than in version 1 (95.45% version 1). As the goal of this experiment was to detect corrupted data readings, these results suggest that HR-Auth works better when the method is called every time an HR message is received from the Bioharness chest sensor (as implemented in version 1). In Experiment 2 the situation was similar as in Experiment 1: in version 2 HR-Auth was invoked faster; however version 1 had a better accuracy in marking data as authentic (86% compared to 72.4%).

4 CONCLUSION AND FUTURE WORK

We described and evaluated HR-Auth, an algorithm to authenticate HR data using two consumer wearables (a smartwatch and a chest sensor). We found that HR-Auth can better authenticate HR data when an HR message is received from the chest sensor. Future work may include the evaluation of HR-Auth under different activities, and the combination of the method with activity recognition.

ACKNOWLEDGMENTS

This research has been supported by the National Science Foundation and the Department of Defense under grant award no. 1560214.

REFERENCES

[1] Denis Foo Kune, John Backes, Shane S. Clark, Daniel Kramer, Matthew Reynolds, Kevin Fu, Yongdae Kim, and Wenyuan Xu. 2013. Ghost Talk: Mitigating EMI Signal Injection Attacks Against Analog Sensors. In *Proceedings of the 2013 IEEE Symposium on Security and Privacy (SP '13)*. IEEE Computer Society, Washington, DC, USA, 145–159. https://doi.org/10.1109/SP.2013.20

[2] David D Luxton, Robert A Kayl, and Matthew C Mishkind. 2012. mHealth data security: The need for HIPAA-compliant standardization. *Telemedicine and e-Health* 18, 4 (2012), 284–288.

[3] Alfredo J Perez, Sherali Zeadally, and Nafaa Jabeur. 2017. Investigating Security for Ubiquitous Sensor Networks. *Procedia Computer Science* 109 (2017), 737–744.

[4] C. C.Y. Poon, Yuan-Ting Zhang, and Shu-Di Bao. 2006. A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-health. *Comm. Mag.* 44, 4 (Sept. 2006), 73–81. https://doi.org/10.1109/MCOM.2006.1632652

[5] Sofia Najwa Ramli, Rabiah Ahmad, Mohd Faizal Abdollah, and Eryk Dutkiewicz. 2013. A biometric-based security for data authentication in wireless body area network (wban). In *Advanced Communication Technology (ICACT), 2013 15th International Conference on*. IEEE, 998–1001.