# AKILLI SAATİNİZ NE KADAR GÜVENLİ?

## HOW SECURE IS YOUR SMART WATCH?

**Murat Karakaya**
Computer Engineering Department
Atılım University
Ankara, Turkey
atila.bostan@atilim.edu.tr

**Atila Bostan**
Computer Engineering Department
Atılım University
Ankara, Turkey
murat.karakaya@atilim.edu.tr

**Erhan Gökçay**
Software Engineering Department
Atılım University
Ankara, Turkey
erhan.gokcay@atilim.edu.tr

Abstract— The Internet of Things (IoT) is a network of devices, vehicles, buildings and other items which are able to collect and exchange data. IoT devices are furnished with technologies such as electronics, software, sensors, actuators, and network connectivity in order to function as desired. A smart watch can be considered as an IoT device as they are equipped by almost all necessary technologies. In essence, smart watches are effectively wearable computers with communications and sensing capabilities. Many mobile apps run over smart watches using a mobile operating system. However, as the other IoT devices they are subject to security issues. In this paper, by surveying and reporting the security concerns and issues at smart watches, we aim to raise awareness on this matter. We also propose a road map for a more secure smart watch platform by defining the responsible actors and their responsibilities.

Index Terms—Smart watch, security, attack, privacy

Özet— Nesnelerin İnterneti (Nİ), bilgi toplama ve bunları kendi aralarında değiştirme imkanına sahip araçlar, cihazlar ve diğer nesnelerin oluşturduğu bir ağdır. Nİ cihazları elektronik, yazılım, sensörler ve ağ bağlantısı gibi teknolojilerle donatılmışlardır. Akıllı Saat sahip olduğu teknoloji nedeniyle bir Nİ cihazı olarak değerlendirilebilir. EN kısa tanımıyla, akıllı saatler algılacılarla ve haberleşme imkanları ile donatılmış giyilebilir bilgisayarlardır. Bir çok mobil uygulama akıllı saatlerin üzerindeki işletim sistemleri sayesinde çalışmaktadır. Ancak, diğer tüm Nİ cihazlarında olduğu gibi akıllı saatler de güvenlik riskleri taşımaktadırlar. Bu çalışmada, akıllı saatlerdeki güvenlik tehditleri ile kaygılarını derleyerek bu konudaki farkındalığı artırmayı hedefledik. Ayrıca, daha güvenli bir akıllı saat teknolojisi için alınması gereken tedbirler ile sorumluları belirleyen bir yol haritası önerilmiştir.

## I. INTRODUCTION

The Internet of Things (IoT) presents a future application area of Internet where users, computing devices, and simple objects embedded with sensing and actuating capabilities cooperate together to provide exceptional ease and economical advantages. Considering the current Internet model, IP-based communication protocols are important in providing the ubiquitous connectivity of IoT devices and applications. Furthermore, the constraints of the sensing platforms such as limited power and reliability require new approaches at communications stack to enable the Internet connectivity. As most IoT applications would entail communications security, some mechanisms must also be designed to provide security [1].

A smart watch is a multi-purpose device that runs computing applications, collects data via its sensors, and communicates with a paring smart phone. Nowadays, smart watches have gained considerable popularity and many different brands of smart watches have been manufactured. According to a latest report, about 21 million smart watches were shipped in 2015 [2]. This popularity can be explained with the increasing capabilities of these devices. In a relatively short amount of time, smart watches have emerged as wearable computers reducing its dependability to smart phones. Now, smart watches are capable of wireless communications (Wi-Fi, Bluetooth, Cellular) and considerable memory and computation power supported with various sensors. Currently, different smart watch brands and types support some set of sensors. These sensors are Accelerometer, Gyroscope, Magnetometer, Barometric pressure sensor, Ambient, temperature sensor, Heart rate monitor, Oxymetry sensor, Skin conductance sensor, Skin temperature sensor, UV sensor, and GPS among others [3]. There are tons of mobile applications developed for exploiting these sensors. For example, more than 4,000 new Android Wear apps were added to the Google Play Store only during last year [4].

As a result of these developments, smart watches can be used to monitor the environment and the user, to collect data, to process them, and communicate the results with remote servers or users as an IoT device. On the other hand, as they become more prevalent, smart watches increasingly store more sensitive information and through connectivity with mobile apps may soon enable physical access functions including unlocking cars and homes.

This survey analyzes existing protocols and mechanisms to secure communications for smart watches as considering them IoT units. We also point out open research issues in this context. We analyze how existing approaches ensure fundamental security requirements and protect communications on smart watches, together with the open challenges and strategies for future research work in the area. This is, as far as our knowledge goes, the first survey with such goals.

## II. SMART WATCH MODEL

A simplified smart watch model is presented at Figure 1. A more detail can be found in [12]. Although there are many different brands and models of smart watches, their essential

internal functionality is fairly alike. They usually contain a low-power embedded processor, a wireless communications interface (Wi-Fi, GSM, or Bluetooth), a mixture of sensors, a power supply, and display. The specific capacity and specifications of these components are designed according to the expected performance and functionality to deliver the users.

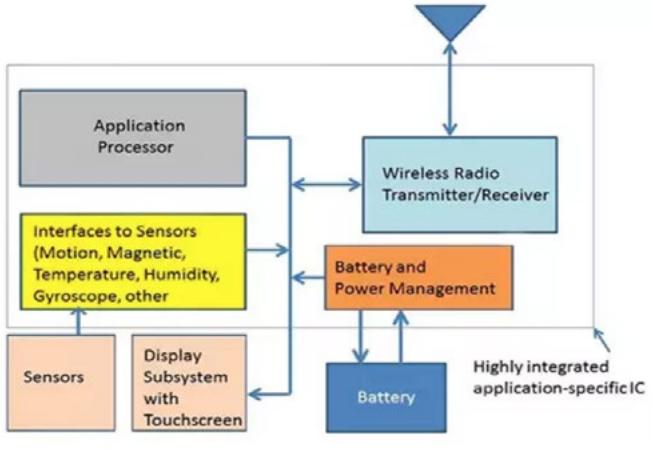


Fig. 1. Smart Watch model (reproduced from [5])

TABLE I. THE RESULTS OF THE HP SECURITY REPORT [9]

| Security Issues | Reported Deficiency |
|---|---|
| Insufficient User Authentication / Authorization | Every smart watch tested was paired with a mobile interface that lacked two-factor authentication and the ability to lock out accounts after 3-5 failed password attempts. Three in ten, 30%, were vulnerable to account harvesting, meaning an attacker could gain access to the device and data via a combination of weak password policy, lack of account lockout, and user enumeration. |
| Lack of transport encryption | Transport encryption is critical given that personal information is being moved to multiple locations in the cloud. While 100% of the test products implemented transport encryption using SSL/TLS, 40% of the cloud connections continue to be vulnerable to the POODLE attack, allow the use of weak ciphers, or still used SSL v2. |
| Insecure Interfaces | 30% of the tested smart watches used cloud-based web interfaces, all of which exhibited account enumeration concerns. In a separate test, 30% also exhibited account enumeration concerns with their mobile applications. This vulnerability enables hackers to identify valid user accounts through feedback received from reset password mechanisms. |
| Insecure Software / Firmware | A full 70% of the smart watches were found to have concerns with protection of firmware updates, including transmitting firmware updates without encryption and without encrypting the update files. However, many updates were signed to help prevent the installation of contaminated firmware. While malicious updates cannot be installed, lack of encryption allows the files to be downloaded and analyzed. |
| Privacy | All smart watches collected some form of personal information, such as name, address, date of birth, weight, gender, heart rate and other health information. Given the account enumeration issues and use of weak passwords on some products, exposure of this personal information is a concern. |

TABLE II. OTHER SECURITY VULNERABILITIES

| Security Issues | Reported Deficiency |
|---|---|
| Recognition of typed data | Using smart watch motion sensors, the typed data can be recognized by malwares [6, 11, 14]. |
| MITM attack | Man-in-the-Middle attack can be executed between smart watch and the paired smart phone [10]. |
| Insufficient Authentication | Authentication via Bluetooth can be exploited to access smart watches [8]. |
| Physically acquiring data | Physically acquiring data from the watches after gaining root access to them is possible as most of the data is stored without any encryption [13]. |
| Recognition of user activities | Gathering and analyzing sensory data, malicious software can predict user activities [16, 17, 18, 19]. |

In the first generation of smart watches, they are assumed to be an extension to the smart phones. Therefore, most smart watches are furnished with Bluetooth 4.0, also known as Bluetooth Low Energy, to connect to a phone. Bluetooth connection requires two communicating parties be in network proximity. On the other hand, at the following generations, most smart phones remove this limitation by having Wi-Fi cards so that when smart watch and smart phone are connected via the same network. Moreover, nowadays, some smart watches contain GSM cards. Thus, advanced smart watches can connect to the Internet directly via 3G or 4G technologies or WIFI. It is probable that in the near future, smart watches will carry on incorporating more wireless technologies such as NFC for payments and other identity-related security mechanisms [12].

## III. SECURITY CONCERNS

Smart watches provide users with watch applications to have access to persistent storage and phone communications. These functions, on the other hand, create a potential security breach for attackers to obtain sensitive data such as position information, text messages, and other private data from the phone [8]. As smart watch capacities of storage and communications increase, these devices become more attractive for attackers [9]. Attacker would abuse smart phone's access to personal data stored in the watch or accompanied smart phone. Thus, users and manufacturers should take precautions when storing information, transmitting personal data, or connecting smart watches into other devices and networks [9].

A study by Hewlett-Packard's HP Fortify showed that all the tested smart watches include noteworthy vulnerabilities related with insufficient authentication, lack of encryption, and privacy concerns [9]. The results of the report from the 10 smart watches tested during the study are provided at Table 1.

In [6, 11, 14], authors show that motion sensors of the smart watch can substantially detect what the user is typing via a keyboard or touch pad by processing motion signal. In [6] authors combine the collected signals with patterns in

English language. In a similar work, the authors investigate the feasibility of keystroke inference attacks on handheld numeric touch pads by using smart watch motion sensors as a side-channel [11]. They propose to employ supervised learning techniques to accurately map the uniqueness in the captured wrist movements to each individual keystroke. Novel keystroke inference models are proposed to mitigate the negative impacts of tracking noises in [14]. In these works, experimental results indicate that using smart watch motion sensors produces accurate predictions [6, 11, 14]. These kinds of applications underline a greater security concern: applications can access to innocent sensors (e.g., accelerometers and gyroscopes) of wearable devices without any access privileges. Preventing such side-channel attacks, in [15] authors propose a novel context-aware protection framework which can be used to automatically stop admission to motion sensors, whenever typing activity is detected.

In [8], the authors investigated a specific smart watch brand closely. They also report the vulnerabilities mainly stem from the underlying Bluetooth protocol. The authors found user authentication as the major problem with the inspected watch since anyone can access the smart watch without any proper permission or any authentication via Bluetooth. The authors propose to enhance authentication process by introducing a two way authentication code [8].

In general, since smart watch mainly use Bluetooth to connect and transfer data to/from smart phone, the security issues related with Bluetooth technology are of high importance. In [10], the authors demonstrate two new Man-In-The-Middle (MITM) attacks on Bluetooth Secure Simple Pairing (SSP). They exploit the falsification of information sent during the input/output capabilities exchange. The authors point out the fact that the security of the Bluetooth protocol is likely to be limited by the capabilities of the least powerful or the least secure device type. In our case, this device is the smart watch. The authors suggest using an additional window at the user interface level. However, as it is noted, this solution can reduce the usability.

In [13], authors propose a methodology for physically acquiring data from the watches after gaining root access to them. The results of the experiments carried on two smart watches indicate that most of the synched data can be recovered. The authors claim that the data such as messages, health and fitness records, e-mails, contacts, events and notifications are accessible directly from the acquired images of the watches. This work shows if an attacker can have the access to a smart phone he can gain considerable amount of stored data. One possible measure to these kind attacks, the data can be stored encrypted at the smart watch.

There are a number of studies which show that by collecting analyzing sensory data, it is possible to predict the user activity with a high accuracy. For example, in [16] authors integrate a smart watch and a smart phone via Bluetooth to recognize three categories of falls (forward, lateral and backward falls). In [17], authors compare with the cases where only one device (the smart phone or the smart watch) is considered to recognize and discriminate the falls. In another work, authors aim to discriminate soft falls from other normal activities [18]. In [19], authors propose a classification scheme to identify running, walking, sitting, standing, jumping, kicking, going-up stairs, going down-stairs, laying, and unknown activities. All these studies indicate that it is possible to predict the user activity by collecting and analyzing the sensory data generated by smart watches. Malicious software can recognize the user activity and share it with its masters.

## IV. DISCUSSION AND CONCLUSIONS

Even though major progress is witnessed during the past decade, smart watch features, uses and design can be considered at their infancy [13]. However, its popularity among consumers and its growing capabilities at computing, storing, and communication are good indicators that new applications will arrive soon. Unfortunately, at the current situation, information and systems security of these smart watches is not the top priority for the manufacturers and the users. As they are prevalent and store large amount of user data, the security will be a greater issue.

TABLE III. A ROAD MAP FOR SECURE SMART WATCHES

| Actor | Possible Actions |
|---|---|
| Smart Watch Manufacturers | • Review security vulnerabilities hardware level<br>• Implement better security mechanisms |
| Operating Systems Developers | • Review security vulnerabilities OS level<br>• Embed and improve security at OS level<br>• Manage and control applications interactions with watch and phone OS<br>• Provide security mechanism to smart watch application developers<br>• Provide secure data transfer, processing, and storing infrastructure |
| Application Developers | • Review security vulnerabilities of developed applications<br>• Provide two-factor authentications<br>• Ensure secure data transfer, processing, and storing at the smart watch |
| End Users | • Aware of security vulnerabilities of smart watches and mobile applications<br>• Do not store or share sensitive data with smart watch<br>• Pay attention to installed applications on smart watch<br>• Activate two-factor authentications at the applications if possible |

In this work, we would like to create an awareness of these issues by pointing out possible security vulnerabilities and recommendations to fix them or to lessen their risks.

In general, the first steps to more secure smart watches

must be taken by manufacturers. They have to work to incorporate necessary security measures into smart watches. However, these measures should be sensitive to the capabilities and capacities of the smart watches. As processing power, storage capacity, and the power supply is considerably limited compared to other mobile and portable devices such as tablets, smart phones, etc., new security techniques or mechanisms should be developed or adopted. Moreover, since smart watches are mostly an extension to the smart watches, they can easily access to sensitive data stored or processed by the phones. As a popular service, the notifications of the applications running on the smart phone are pushed to smart watches. GPS location data of the smart phone is accessible easily. Thus, an application running on a smart watch can be a back door to the smart phone. So new type malwares targeted to the smart watches can be developed soon to capture the data stored, processed, or generated on the smart phones.

Thus, all above considerations imply the responsibility of smart watch manufacturers and Operating System developers for making this platform more secure. The next actors are the application and protocol developers. Even though the application market of smart watches are relatively small compared to that of smart phones, there are thousands of applications available for serving a variety of user services. The simplest form of these applications are forwarding notifications occurred at the smart phone to the associated smart watches. Other service type is to provide simplistic interface to the phone applications with limited features. Last service type of these applications can be classified as the management of phone features via smart watch display. For example, GPS can be turned on via voice recognition system messages can be created and sent using the phone services. The vulnerabilities discussed in the paper can be exploited by the malwares to collect or modify the data processed by other applications. Insufficiency in security at cloud access mechanisms, for example, can be exploited to access the cloud account of the smart watch owner. Thus, application developers must check their interaction between phone and cloud services considering security issues.

Next, smart watch users should consider security when choosing a smart watch and a mobile application. First of smart watch owners must be aware of these security risks. Users are recommended not to enable sensitive access control functions such as car or home access unless strong authorization is provided [9]. Applications should provide 2-factor authentication technology for user certification [7].
As a future work, we plan to work on identifying specific security vulnerabilities in communication protocols such as Bluetooth and WIFI. As most of the IoT devices depend on wireless communications, the protocols should be examined and enhanced for providing secure data communications to such devices. Direct implementation of existing security measures such as authentication or encryption may not be feasible since the limited resources owned by the smart watches and other IoT devices. Therefore, we consider the adaptation of security mechanisms to smart watches as a good start to this direction.

## REFERENCES


[1] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues."IEEE Communications Surveys & Tutorials 17.3 (2015): 1294-1312.

[2] IDC Press Release, "IDC Forecasts Worldwide Shipments of Wearables to Surpass 200 Million in 2019, Driven by Strong Smartwatch Growth", https://www.idc.com/getdoc.jsp?containerId=prUS40846515, accessed July, 2016.

[3] J. Phillips, The 10 most likely sensors in a 10-sensor Apple smartwatch, http://www.pcworld.com/article/2366126/the-10-most-likely-sensors-in-a-10-sensor-apple-smartwatch.html, accessed July, 2016.

[4] R. Temple and J. Naziri, "40 best Android Wear apps in 2016" in Techradar, http://www.techradar.com/news/wearables/best-android-wear-smartwatch-apps-2015-1281065, 2016.

[5] D. Bursky, "Wireless Connectivity Lets Smart Watch Users Communicate and Monitor Themselves", http://www.digikey.com/en/articles/techzone/2014/oct/wireless-connectivity-lets-smart-watch-users-communicate-and-monitor-themselves, 2014.

[6] Wang, He, Ted Tsung-Te Lai, and Romit Roy Choudhury. "Mole: Motion leaks through smartwatch sensors." Proceedings of the 21st Annual International Conference on Mobile Computing and Networking. ACM, 2015.

[7] Cha, Byung-Rae, et al. "Design of Micro-payment to Strengthen Security by 2 Factor Authentication with Mobile & Wearable Devices." Advanced Science and Technology Letters, Vol.109 pp.28-32 (2015).

[8] Razaque, Abdul, et al. "Pebble Watch security assessment." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2016.

[9] HP Fortify, "Internet of Things Security Study: Smart watches", http://go.saas.hpe.com/fod/internet-of-things, 2015.

[10] Haataja, Keijo, and Pekka Toivanen. "Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures." IEEE Transactions on Wireless Communications 9.1 (2010): 384-392.

[11] Maiti, Anindya, et al. "(Smart) watch your taps: side-channel keystroke inference attacks using smartwatches." Proceedings of the 2015 ACM International Symposium on Wearable Computers. ACM, 2015.

[12] Steck, Ken, and Hansheng Tan. "Transformation of the Digital Watch: The evolution and what it signals." IEEE Consumer Electronics Magazine 5.1 (2016): 89-92.

[13] Baggili, Ibrahim, et al. "Watch what you wear: preliminary forensic analysis of smart watches." Availability, Reliability and Security (ARES), 2015 10th International Conference on. IEEE, 2015.

[14] Liu, Xiangyu, et al. "When good becomes evil: Keystroke inference with smart watch." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.

[15] Maiti, Anindya, et al. "Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms." Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016.

[16] Casilari, Eduardo, and Miguel Ángel Oviedo-Jiménez. "Analysis of a hybrid Android system for fall detection." (2016).

[17] Casilari, Eduardo, and Miguel A. Oviedo-Jiménez. "Automatic fall detection system based on the combined use of a smartphone and a smartwatch."PloS one 10.11 (2015): e0140929.

[18] Genoud, Dominique, Vincent Cuendet, and Julien Torrent. "Soft Fall Detection Using Machine Learning in Wearable Devices." 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2016.

[19] Pham, Cuong. "MobiRAR: Real-Time Human Activity Recognition Using Mobile Devices." Knowledge and Systems Engineering (KSE), 2015 Seventh International Conference on. IEEE, 2015.