POSTER: Watch Out Your Smart Watch When Paired

Youngjoo Lee
Yonsei University
Seoul, Korea
yj.lee91@yonsei.ac.kr

WonSeok Yang
Yonsei University
Seoul, Korea
zmsenqn@yonsei.ac.kr

Taekyoung Kwon[*]
Yonsei University
Seoul, Korea
taekyoung@yonsei.ac.kr

ABSTRACT

We coin a new term called *data transfusion* as a phenomenon that a user experiences when pairing a wearable device with the host device. A large amount of data stored in the host device (e.g., a smartphone) is forcibly copied to the wearable device (e.g., a smart watch) due to pairing while the wearable device is usually less attended. To the best of knowledge, there is no previous work that manipulates how sensitive data is transfused even without user's consent and how users perceive and behave regarding such a phenomenon for smart watches. We tackle this problem by conducting an experimental study of data extraction from commodity devices, such as in Android Wear, watchOS, and Tizen platforms, and a following survey study with 205 smart watch users, in two folds. The experimental studies have shown that a large amount of sensitive data was transfused, but there was not enough user notification. The survey results have shown that users have lower perception on smart watches for security and privacy than smartphones, but they tend to set the same passcode on both devices when needed. Based on the results, we perform risk assessment and discuss possible mitigation that involves volatile transfusion.

KEYWORDS

wearable device; data extraction; data transfusion; risk assessment

1 INTRODUCTION

Wearable computing devices are "miniature" electronic products worn by users and so in general they are lack of a conventional user interface and a wide network connectivity. For example, Apple Watch provides a "38 or 42mm" force touch display and a tiny crown along with haptic engines, sensors, Bluetooth, and Wi-Fi in ad-hoc mode for interactions only in near range. Therefore, wearable computing devices require a host device, such as a smartphone, for their connectivity, functionality, and usability to be enriched.

First of all, a personal wearable device must be initially paired to the host device for new device initialization and personalization — this process is called a pairing. For instance, a user initially needs to pair a maiden smart watch to his smartphone through a Bluetooth or NFC channel before use. The smart watch is then allowed to communicate with the paired smartphone for further data updates and backups while in use, e.g., SMS notification, weather forecast update, and health record backup, even without requiring user consciousness on the paired connections. Now both devices may need to be attended at the same level.

In this paper, we deal with data security problems that can occur in device pairing of smart watches, and coin a new term called *data transfusion.* We approach the problems in two-fold study design. First we perform an experimental study to extract data from smart watches paired with a smartphone in different phases. We consider three popular platforms such as Android Wear, watchOS, and Tizen in our experiments. Second we conduct a survey study to understand user perception and behavior with regard to the so-called data transfusion. Based on these studies, we perform risk assessment on smart watches and discuss how to reduce the risk.

There have been several previous works that manipulated data extraction of smart watches from forensic perspectives. They include Do et al.'s work, respectively, on Samsung Galaxy Gear [2], and Baggili et al.'s work on Samsung Galaxy Gear2 Neo and LG G Watch [1]. Compared to the elegant previous works, our study is more uniquely focused on exploring the phenomenon called data transfusion (saying, not only extracted data) by concrete experiments accompanying user surveys and risk assessment. To the best of our knowledge, this is the first work to arise such implication.

2 THREAT MODEL - DATA TRANSFUSION

Our main focus is on what happens in a wearable device due to pairing. For initialization and personalization, the devices need to exchange necessary data and particularly the data stored in the host device that belongs to a user. As for such data transferred from the host device, we set the following definitions.

Definition 2.1. Device pairing is a process that sets up an initial linkage between a wearable computing device and a host device to allow further reciprocal interactions, and it necessarily accompanies a data exchange between those devices.

Definition 2.2. Data transfusion is a phenomenon that is caused by a device pairing — the host device infuses a copy of its (locally stored) secret and/or private user data into the paired wearable device to serve further paired actions.

The following threat model then raises research questions under data transfusion. *An adversary who acquired a user's wearable device, e.g., a smart watch, could have a chance from it to obtain user's secret and/or private data that might also be stored in a host device, i.e., a smartphone.* What kind of data could be found on the fly and how secret and/or private are they? Do those devices provide an unlock mechanism in the same degree of security? If they aren't, it may intrinsically be a great problem. But if they are, we may tackle another threat. *An adversary who also acquired a user's host device, could have a chance from the wearable device to find user's behavioral characteristics originally observed in the host device.* For

[*] Corresponding author.

CCS'17, Oct. 30–Nov. 3, 2017, Dallas, TX, USA.

ISBN 978-1-4503-4946-8/17/10.
DOI: https://doi.org/10.1145/3133956.3138831

Table 1: Experimental setup: types of pairing devices

Wearable Devices	Host Devices
Sony SmartWatch3 (Android Wear 1.3) LG G Watch (Android Wear 1.4)	LG Nexus 5X (Android 7.0)
Samsung Galaxy Gear (Tizen 2.2.1.1) Samsung Galaxy Gear2 Neo (Tizen 2.2.1.2)	Samsung Galaxy S3 (Android 4.3)
Apple Watch (WatchOS 3.1)	Apple iPhone 6S Plus (iOS 10.1.1)

Table 2: Experimental results of data transfusion

Data \ Platform	Android Wear	Tizen	watchOS
Encrypted Lock Pattern	□ □ ■	⊠ ⊠ ⊠	⊠ ⊠ ⊠
Contact	■ ■ ■	■ ■ ■	■ ■ ■
SMS/MMS/Messenger	■ ■ ■	□ ■ ■	■ ■ ■
E-mail	□ ■ ■	□ ■ ■	□ ■ ■
Memo	□ ■ ■	⊠ ⊠ ⊠	⊠ ⊠ ⊠
Wi-Fi SSID/Password	■ ■ ■	⊠ ⊠ ⊠	⊠ ⊠ ⊠
Photo	■ ■ ■	■ ■ ■	□ □ □
Fitness Data	■ ■ ■	□ ■ ■	□ □ □
Location	□ □ ■	⊠ ⊠ ⊠	⊠ ⊠ ⊠
Calendar	□ ■ ■	□ ■ ■	□ □ ■
Host Device Info.	⊠ ⊠ ⊠	■ ■ ■	⊠ ⊠ ⊠
Host Installed Apps	■ ■ ■	⊠ ⊠ ⊠	□ ■ ■

□: Not transfused, ■: Transfused, ⊠: Unavailable
Three squares represent phase t_1, t_2 and t_3 for each platform

instance, does a user set the same passcode to unlock both devices? If the user does, a resource-limited wearable device could be a good medium target to attack the host device. An adversary could have at least double the chance of guessing a passcode. Finally we are also wondering if users are properly notified and aware of such phenomena and threats.

3 EXPERIMENTAL STUDY

Experiment Setup and Design. We conduct an experimental study of data extraction considering data transfusion in actual user environments. As summarized in Table 1, we attempt to extract stored data from five smart watch models, respectively, operated in three different platforms (Android Wear, watchOS, Tizen). In more concrete, we extract data in three subsequent phases of device connections: t_1, t_2, and t_3. At phase t_1, we disable network interfaces and isolate the smart watch to see data transfusion right after the initial pairing process. At t_2, we let the smart watch connected to the host smartphone to see data transfusion in the basic user mode. At t_3, we install additional apps to the smartphone and smart watch to see data transfusion in more complex use cases.

Experimental Results. In the experiment, we were able to extract various kinds of transfused data from smart watches at different phases. Table 2 illustrates the results of data transfusion at each phase according to the types of platforms. We also tried to observe whether enough notification was given for data transfusion.

To extract data from SmartWatch3 in Android Wear, it was possible to boot into recovery or bootloader mode without submitting a lock pattern although SmartWatch3 was locked by the lock pattern. We were able to observe transfused data even from t_1 without solid notifications or warnings. None of the retrieved files except for the pattern lock file were encrypted, and it was possible to analyze them with text and hexadecimal editors only. In watchOS, we externally observed the data transfusion phenomenon as a user because it was unable to bypass the locked state. In Tizen which was default in unlocked state, interestingly, the same transfusion results were observed at t_2 and t_3, respectively. This was because Tizen did not store the data from additionally installed apps.

To be specific, we extracted user's own Contact information and SMS/MMS messages which have a high risk score according to the risk assessment in Section 5. Also, we extracted Wi-Fi connection information such as Wi-Fi SSID, Wi-Fi password and encryption type (WPA-PSK). Some sensitive data that were never used by the smart watch but rather used by the paired smartphone was leaked from the smart watch. Especially, we retrieved encrypted lock pattern from SmartWatch3 which was cryptographically hashed by SHA-1. We were able to disable the pattern lock authentication simply by deleting the file in custom recovery mode. Once deleted, SmartWatch3 did not request users to unlock the lock pattern any more. Furthermore, we were able to crack the hashed lock pattern by generating a rainbow table with a simple Python script [4]. This implicates that the host smartphone paired to this smart watch could also be unlocked if users set the same lock pattern on both devices.

Moreover, we observed data transfusion from additionally installed fitness app called Strava. We observed fitness logs such as time, speeds, distance, accuracy data in clear text.

4 SURVEY STUDY

Survey Design and Study Method. The aim of our survey is to empirically understand how users think about data transfusion phenomenon. For survey, we point out research questions that satisfy our purpose.

(1) Is there any difference in users' security and privacy related perception on smart watch compared with smartphone?

(2) Have users seen the notification message that indicates transferring of the information? And does it affect users awareness of data transferring, effectively?

(3) Do users set the same passcode for both smartphone and smart watch?

We strive to recruit 205 participants (189 self-identified as male and 16 as female) who use both smartphone and smart watch. We validate actual smart watch users by requiring users to take a picture of the message that we sent. The model of the smart watches consists as follows: 49% of Samsung gear users, 43% of Apple Watch users and 8% of others. We present what we observed and analyzed in the following subsections.

Lower Risk Perception on Smart Watch. To obtain quantitative and qualitative understandings of how users' risk perception vary across smartphone and smart watch, we compare participants' risk perception of smart watch to that of smartphone in three perspectives: awareness of data storing, awareness of data leakage and awareness of security threat when lost. All three results show lower percentage on a smart watch than that of smartphone which indicate that users have lower risk perception on a smart watch.

Moderate Perception on Data Transfusion. It is necessary to have notification messages that indicate some sensitive data such as contact list, call records and GPS data in a smartphone can be transferred to a smart watch when paired. Apple, Sony and LG watch inform users with notification message but Samsung Gear does not. We separated participants into this two groups and asked *if they have seen the notification message.* Among the users who use smart watch with notification message, only 50% answered that they have seen it. And, 57% of the users whose smart watch lacks the notification message answered that they have seen the notification message. This results can be implied that whether the smart watches have notification or not, it does not affect the users. Furthermore, 85.2% of people who are aware of data transfusion initially were also aware of it when in use. Initial awareness plays significant role in continuous awareness, putting more weight on a high necessity of well-defined notification on a smart watch from the initial pairing process.

User's Behavioral Practice Different from User Perception. Based on the results showing that users tend to have lower risk perception on smart watches than smartphones, we expect that users set the different passcode for respective devices. However, users tend to set the same passcode on both devices and do not behave as they perceive. When we asked participants to answer *if they actually use or will use the same passcode on both a smartphone and a smartwatch*, 78% of participants who are using the same locking method on smartphone and smart watch actually use the same passcode on both devices. User's actual behavior seems to be far below their awareness and there is a gap between perceived risk and the actual risk.

5 RISK ASSESSMENT

From the experimental results, we observed that sensitive data are transfused from a smartphone to a smart watch. Subsequently, we perform risk assessment of smart watch data by considering the transfused user-specific data as an asset [3]. Firstly, we classify data into four categories according to the context of data: controls of device, communications, sensor data and user written data. Secondly, we define data and assign the impact score in terms of security and privacy. Lastly, we calculate the risk score by multiplying the impact score and the likelihood score of transfused data as follows.

$$Risk_{platform}(data) = Impact(data) * Likelihood_{phase}(data) \tag{1}$$

As the data to be transfused are different according to the transfusion phase, to reflect this, we scored the points that are likely to be transfused for each data as likelihood score. The likelihood, since we experimented independently on different platforms, must be a value that is different according to the platform. The sum of the risk score at t_3 is as follows on each platform: Android Wear - 78, Tizen - 65 and watchOS - 49. Figure 1 shows the risk score of transfused data on each platform at t_3.

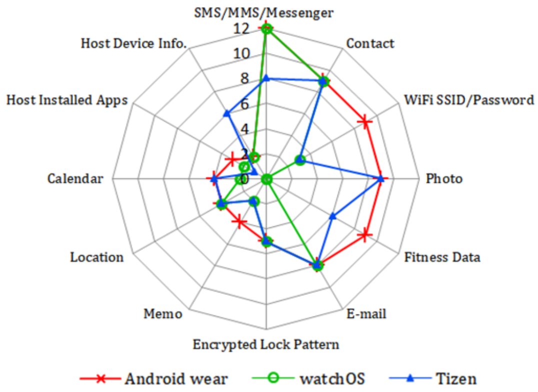

Figure 1: Risk scores of transfused data in each platform

6 DISCUSSION AND MITIGATION

We conducted both experimental and survey studies with regard to data extracted from smart watches by focusing on the data transfusion phenomenon, and performed risk assessment. We observed that rare notification lowered user perception on data transfusion and could be a trigger of security or privacy related incidents. For mitigation, if a smart watch is isolated, we propose transfused data to be removed from the smart watch after a certain amount of time according to *the descending order of the priority*, that is, from the highest priority based on our risk assessment levels shown in Figure 1. When the original user returns and wears the smart watch again, the removed data is re-transfused. We call this strategy *volatile transfusion* that enables safe data elimination when the device is separated from its user or the host device. We also propose to provide an explicit notification message to the user regarding data transfusion of the high priority data. It would also be considerable to request a user's active response, e.g., by swiping the items to be transfused. Future work may include a longitudinal user study adopting suggested mitigations with simulation experiments. We expect to observe how users react and compromise between usability and security when using smart watches.

ACKNOWLEDGMENTS

This work was partly supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. NRF-2 015R1A2A2A01004792), and also by the MSIT under the ITRC (Information Technology Research Center) support program (IITP-2017-2012-0-00646) supervised by the the IITP (Institute for Information & communications Technology Promotion).

REFERENCES

[1] Ibrahim Baggili, Jeff Oduro, Kyle Anthony, Frank Breitinger, and Glenn McGee. 2015. Watch what you wear: preliminary forensic analysis of smart watches. In *ARES Conference Proceedings*. IEEE, 303–311.

[2] Quang Do, Ben Martini, and Kim-Kwang Raymond Choo. 2017. Is the data on your wearable device secure? An Android Wear smartwatch case study. *Software: Practice and Experience* 47, 3 (2017), 391–403.

[3] I ISO and I Std. 2011. Iso 27005: 2011. *Information technology–Security techniques–Information security risk management. ISO* (2011).

[4] Michael Spreitzenbarth. 2012. Cracking the Pattern Lock on Android. (2012). https://forensics.spreitzenbarth.de/2012/02/28/cracking-the-pattern-lock-on-android/