Wear it or share it? Wearables and security.

By Charalampos Z. Patrikakis and George Loukas

Miniaturization in electronics has been the ground over which ubiquitous and pervasive computing has grown, squeezing the telephone and the computer, first into a pocket sized device, and now into wearable (and sewable) devices. Though these latter devices may require the presence of a mobile device, to which they are tethered, in many cases they are even able to operate autonomously, offering full communication and processing capabilities equal to that of a mobile phone. Regardless of their capabilities for autonomy, there is a common factor which characterizes wearables: Sensing capabilities. From biometric to motion and location sensors, wearable devices are capable of understanding the location, status, even condition and mood of their owner.

This knowledge can prove extremely important and useful in personalizing the use of mobile devices. There are many reasons why one would choose a wearable over a traditional mobile device. First, there is the advantage of using sensors able to take biometric measurements in a manner that is far easier than would be possible with a mobile device, especially for heartbeat, skin conductivity and transpiration. For instance, a mobile device may take heart beat measurements using the flash light, which is considerably less accurate than the measurements obtained via a sensor.

Second, there is the “wearability” *vs.* portability aspect. While a wearable device is always on the wearer’s body, and in most cases in a location where it can take the appropriate measurements even without the user’s intervention (such as on the wrist for heart rate or gestures), a mobile device is usually in one’s pocket, and needs to be taken out and activated before taking measurements.

Another important issue is feedback. While a wrist-worn device can notify the user about an event through a vibration which is difficult not to notice, a similar notification through vibration on a mobile device, in a pocket or elsewhere, may go unnoticed. Finally, there is the issue of ubiquity. With more wearables becoming water proof, you can simply have your device with you, practically everywhere, while forgetting it when leaving home is far rarer than forgetting your mobile phone. After all, a wrist watch has been around at least one hundred years before the first mobile phone, and in a similar shape and weight to its wearable successor of today.

Let’s take a look at a couple of practical examples of the superior availability and therefore usefulness of wearables over mobile devices. First of all, the recent introduction of the Pokemon Go app for wearables. Game players who have had the chance to download the watch app can appreciate how easy it is to simply tap the screen of the watch, following a light wrist vibration notification, as compared to having to remove a phone from your pocket (if you have felt the vibration), tap the pokestop and then swipe your finger to the screen.

Our second and more interesting example comes out of the TRILLION project [TRILLION] on community policing. In the project, several scenarios on community policing were selected for the pilot trials, including reporting on antisocial behavior, domestic violence, or asking assistance from firefighters or the police. Though the use of a mobile device app offers a comprehensive set of capabilities and reporting options to the user, one must consider several factors that could affect the use of a mobile app, with stress being at the top of the list. Imagine running to get away from a fire in a building. Would you have the time or be composed enough to find and activate your phone, select the app and ask for help or report the event? On your wearable device, all it would take (even while running away from the fire), is to lift your arm and click a side button to open the app (i.e. in the form of a glance in an apple watch). Safety is another important factor. How safe would you feel, getting your mobile phone out of your pocket to report a group of hooligans smashing cars across the street, as compared to using your watch app, in a similar way as before? And how easy would it be for you to go unnoticed while doing it?

It is fairly safe to assume that as context awareness over the processing of sensor data from one's wearable device improves, the cases where a wearable device will prove more useful will increase in number. However, the greater the dependence on wearables, the greater also the need to address the associated security and privacy risks.

As embedded systems with wireless connectivity, most wearables inherit many of the known security issues found in mobile and wireless devices. For example, they can be infected with malware and the network traffic they receive and generate can be vulnerable to eavesdropping or manipulation, just as with any other wireless computing device. In 2015, a researcher demonstrated a partly theoretical proof-of-concept attack exploiting a FitBit Flex vulnerability via Bluetooth to get the device to infect with malware any computer paired with it from then on [Paulli2015]. Fake firmware updates may manipulate the sensor data transmitted, drain the battery so as to render it unavailable, etc. In addition, location tracking used for device activation and supported by a multitude of IFTTT recipes for controlling thermostats, garage doors and other devices, can also be valuable information for burglars. Still, all these are nothing new in the space of the Internet of Things and cyber-physical attacks [Loukas2015]. What makes wearables different is the extent to which a security or privacy breach can affect the users themselves. A 2016 report published by the IEEE Center for Secure Design identified 25 different attack scenarios involving a simple fitness tracker [West2016].

The standard type of wearable is one that collects data of at least some direct or indirect relevance to physical privacy (where I am and what I am doing), emotional privacy (how I feel) and health privacy, such as sleep patterns, heart rates, stress levels, types of activity, and all this on a 24/7 basis. The data are typically transmitted via Bluetooth or other low-energy short-range wireless technology to some sort of a mobile device or other computing system and from there to a cloud service for the user to be able to access from anywhere and at any time. The unprecedented range and quantity of data collected about the human being that wears the device means that unscrupulous use (e.g., for health insurance purposes) and poor security measures to protect the data from hackers, especially if that cloud service goes out of business, are realistic risks. In fact, in almost all practical cases, wearing means sharing, usually through a cloud service. And the data collected via wearables are almost never the types of data that one would consciously prioritize for sharing.

One could expect that information of such extraordinary value requires extraordinary effort in protecting it, and this is certainly not the case yet. This being a relatively new battleground for smart device manufacturers, it is all about lowering costs and introducing highly-marketable features. Introducing strong security is very rarely a priority, and it is also a technological challenge due to the wearables' relatively limited processing, energy and network resources. The same security and privacy problems are anticipated in other areas beyond fitness tracking and health monitoring. The more useful wearables become in policing, defense, access control and other crime-relevant applications, the greater the interest of criminals in exploiting the weak security afforded on these devices.

One way of combating the fears around privacy is the use of anonymity ensuring techniques. Such techniques have been successfully used in reporting illegal or criminal behavior, ensuring that the reporting person remains anonymous and avoiding the fear of any consequences (involvement in a trial process or vigilante actions by offenders). Several organizations globally, such as Crimestoppers international [Crimestoppers], or the police have been using tools and platforms allowing for anonymous reporting using web forms, applications or even short messages.

In the case of personal data reporting, involving anonymity in the data transmission process may seem controversial: How can you anonymize the transmission of your personal data? A solution proposed by the TRILLION project [TRILLION] is the use of a two step anonymization process, making use of both anonymization and encryption techniques, in order to make sure that the transmitted information is made available in the correct form to all involved parties in the data reporting/analysis process. The process involves the encryption of information using public key cryptography, allowing safe communication between the data owner (user) and the data processor (entity receiving the data and responsible for processing it). Between these two entities, an intermediate proxy (which could be operated by a third party), is responsible for hiding the identity of the reporter, substituting the real ID of the user with a hash number; the latter could be unique per communication attempt. In this way, the data processor is only aware of the data (but not the ID of the data owner), while the intermediate proxy, though aware of the ID of the data owner, is unaware of the content of the communication.

Of course, such schemes imply trusting all involved parties in this communication process, since the combination of communication proxy and data processor logs could endanger anonymity. However, the successful operation of anonymous reporting schemes globally has proven that the proposed scheme could work. Furthermore, use of encryption techniques which involve the use of attributes in the decryption process (such as Attribute Based Encryption), could also be deployed in ensuring that access to all or parts of the information is provided only to individuals or entities with a particular profile (such as your personal doctor, or a hospital, but not an insurance agent).

In conclusion, as the amount of data generated by personal devices is increasing, supported by the trend of making these devices more personal (wearable, sewable), so too will the risks of personal privacy violation increase. It is important that privacy by design approaches, incorporating both data encryption and data anonymization techniques are followed, since earning trust is of utmost importance when you ask end users to “wear and share”.

References

[TRILLION] TRILLION: TRusted, CItizen - LEA colLaboratIon over sOcial Networks, funded under call H2020-FCT-2014, REA grant agreement n° [653256].

[Paulli2015] Paulli, Darren (2015). '10-second' theoretical hack could jog Fitbits into malware-spreading mode. The Register. http://www.theregister.co.uk/2015/10/21/fitbit_hack/

[Loukas2015] Loukas, George (2015). Cyber-physical attacks: A growing invisible threat. Elsevier.

[West2016] West, J., Kohno, T., Lindsay, D. and Sechman, J., 2016. Wearfit: Security design analysis of a wearable fitness tracker. Tech. Rep., IEEE Center for Secure Design.

[Crimestoppers] Crime Stoppers nternational. URL: http://csiworld.org/