Abdulraheem Mansur
Dr. Peng Li
ICTN4040 601
4/10/17

Security Concerns of Wearable Technology

Wearable technology has grown extremely popular. From smartwatches to glasses, there are a variety of wearables that are now available to consumers for various purposes. Most consumers purchase these devices for ease of data access. Smartwatches may be used to avoid having to pull out their phone to collect basic information such as the weather forecast or to quickly read a text message or calendar reminder. Activity trackers help one improve on their workout and assist in tracking performance over time. Smart glasses allow us to better document our trips and experiences to help share with friends and family. So what happens to the data collected by wearables? Consumers generally use it for the intended purpose, but what else could come from it? Are consumers the only ones that use these types of devices? Who else could access this data? Is the data transmitted securely? Is the data just public consumer information or is there a possibility that private consumer or company information may be at risk? As we physically come closer to technology there are even larger efforts to integrate man and machine, but what are the impacts?

Data collected by wearables are generally stored locally on the device and then transmitted to a mobile device of sorts (most commonly a mobile phone) as an intermediary before reaching its final destination, the cloud. Securing the wearable devices is becoming more common but many can be accessed without any type of authentication. Having physical access to a device generally allows you to circumvent most of the security protocols that are in place. At a recent

Black Hat conference Symantec’s Threat Researcher Candid Wueest “brought to the forefront the reality that wearable device developers do not even think about how to approach the security issue when the developing process starts. The overall consensus is to get the device ready to be produced and then “sprinkle some security on top” in the end.” This unfortunately is not unique only to the wearables market. Although developers have improved, many applications approach security in this way. Requiring some level of authentication would help improve authorized access. Encrypting the data on the wearables and implementing data wipes upon unsuccessful access attempts would then help keep the owners information confidential. Building security into the software for these devices from day one will help to secure the data that is stored on the devices. Developing a secure means of transmitting this information to its base smart phone or tablet also helps to ensure the data is not compromised when being synced.

Most wearables use Bluetooth and/or Wi-Fi technology to communicate with the base device. According to ITBuesinessEdge “Recently, security firm BitDefender demonstrated that the Bluetooth communication between Android devices and smartphones could be deciphered using brute-force attacks.” These were used to access data communicated between the devices. Alternatively, Bluetooth can be used to gather real-time data on individuals as well. Wired featured an article detailing an example of this at a recent Black Hat conference. “After explaining to the Black Hat public that he actually had his self-manufactured Raspberry Pi device “sniff” (track) up to at least 6 jawbone and Fitbit devices from visitors at his speaking session. He showed the public how easy it was to find out people’s whereabouts, their listed hardware addresses and the time they actually left or entered the room. The security breach that Wueest demonstrated was quite clear." This type of information would be most appealing to marketing and advertising companies to gauge trends and interest in products anywhere such as a mall or shopping center. These devices could be mounted on anything from dividers to clothes racks and we would be completely unaware of any "intrusion". With some devices, the software is set to detect changing environments such as the Dual Blink device, which are "glasses-mounted devices that track the wearer's blink rate and, upon absent blinks, trigger blinks through actuation: light -ashes, physical taps, and small puffs of air near the eye. Although this may have limited impact, the software could be tampered with if not secured properly to cause discomfort to the users eyes instead of providing relief. As Selena Larson mentioned that the FDA confirmed Cardiac devices to have vulnerabilities and although this isn't considered a wearable, it shows just how vulnerable we can become once we integrate with technology.

Once the data has landed on our mobile phone or tablet, it is eventually synced to the cloud for storage and to be data mined to present the information to the user for its intended purpose. However, companies may sell this information to 3rd parties such as insurance companies or consumer product lines for health or weight loss management. Outside of our actual health information our photos could show our travel history and with that, what type of risk we pose to exposure of certain infections around the world. All of the information can be used to help track outbreaks and to contain them. However, it could also be used to increase premiums for individuals that like to travel the world. A recent article by Teena Maddox shows that "As more consumers purchase wearable tech, they unknowingly expose themselves to both potential security breaches and ways that their data may be legally used by companies without the consumer ever knowing." This covers only the legal aspects of data collected. What happens when the organization legally storing your data is compromised in some fashion? As Teena Maddox stated "If that data was carelessly stored, and then stolen through a data breach by a malicious third party and sold to unscrupulous organizations that want to use that data to assess your health risks, you could one day face steep increases in health insurance, or even a policy cancellation." As we know, policies change and the standards that we have for maintaining health care can be impacted. Would we want our health care status to be impacted by information collected on a wearable device? I believe most would not. Devices such as the FootStriker can detect if you are a heel striking runner or a forefoot striker runner. Will the accuracy of the device be taken into consideration when determining our health status? Will different types of runners have to pay different premiums? Regardless, the analysis shifts away from the broader health evaluation and more towards the reliance on data from the wearable source.

So what data is actually collected? Depending on the type of device, it can be anything from biometrics to where you dined for lunch. What happens when you inadvertently capture sensitive information of your own with smart glasses and it's transmitted and posted to the cloud? What if the sensitive information isn't yours? It could be the personal information of another individual or intellectual capital of your employer. Who remains liable for the breach? The ability to track this data and understand who has accessed it and remove it still remains a huge challenge. Once it posts to the public, there are numerous means for the information to be captured and stored and then retransmitted even if removed from its original source. A report was recently published by researchers at the American University and Center for Digital

Democracy stating “The connected-health system is still in an early, fluid stage of development,” explained Kathryn C. Montgomery, PhD, professor at American University and a co-author of the report. “There is an urgent need to build meaningful, effective, and enforceable safeguards into its foundation.” Once this information is found to be exposed, there is still work to understand who will be held responsible and what will be enforced to prosecute guilty parties. Criminals will no doubt try to take advantage of this system as well and will be sure to manipulate it to avoid being charged for any wrong doing. Keeping our personal data hidden will continue to pose a challenge. Tools such as encryption will continue to be needed to protect personal data. Companies will need to enforce strict policies on what types of devices are allowed in specific situations such as internal meetings or anything related to intellectual capital that may give them a market edge with competitors. Although trusted policies will be enacted, many companies may use similar means of detecting wearable users much like the marketing and advertising units, allowing them to enforce strict policies in certain venues.

Although many benefits can be derived from wearables, securing them should be of the utmost importance with their development. There are a number of third parties that would love to have as much information as possible on our health and wellbeing. Unfortunately they are not considering our best interest. Therefore we must be vigilant in what devices we use and understanding what data we provide when using them, who has access to this data, and what steps we can take to protect ourselves should this data be mishandled or compromised. As much as technology can assist us, we don’t always understand the long-term implications of its use on our overall care. More attention should be brought to this issue by us (the users) to ensure that our concerns are properly addressed by legislation and standards to ensure our information is used for its intended purpose and not for the profit of an unknown third party.

References

Artem Dementyev and Christian Holz. 2017. DualBlink: A Wearable Device to Continuously Detect, Track, and Actuate Blinking For Alleviating Dry Eyes and Computer Vision Syndrome. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 1, 1, Article 1 (March 2017), 19 pages. *
DOI: https://doi.org/10.1145/3053330

Mahmoud Hassan, Florian Daiber, Frederik Wiehr, Felix Kosmalla, and Antonio Krüger. 2017. FootStriker: An EMS-based Foot Strike Assistant for Running. Proc. ACM Interact. Mob. Wearable Ubiquitous Technol. 1, 1, Article 2 (March 2017), 18 pages. *
DOI: https://doi.org/10.1145/3053332

ITBusinessEdge, "Five Potential Security Concerns Related to Wearables"
http://www.itbusinessedge.com/slideshows/five-potential-security-concerns-related-to-wearables.html

Ogunkoya Yewande, "New Report: Health Wearable Devices Pose New Consumer and Privacy Risks" Center For Digital Democracy, 15 December 2016
https://www.democraticmedia.org/CDD-Wearable-Devices-Big-Data-Report

Maddox Teena, "The dark side of wearables: How they're secretly jeopardizing your security and privacy" TechRepublic
http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy/

Napel Mano ten, "Wearables and Quantified Self Demand Security-First Design"
https://www.wired.com/insights/2014/10/wearables-security-first-design/

Larson Selena, "FDA confirms that St. Jude's cardiac devices can be hacked" CNN, 9 January 2017
http://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/

Kharpal Arjun, "Elon Musk: Humans must merge with machines or become irrelevant in AI age" CNBC, 13 February 2017
http://www.cnbc.com/2017/02/13/elon-musk-humans-merge-machines-cyborg-artificial-intelligence-robots.html