*Deliverable 0*

Tino Pimentel

Computer Science Department

College of Charleston

Charleston, SC USA

[pimentelta@g.cofc.edu](mailto:pimentelta@g.cofc.edu)

Alexander Laughlin

Computer Science Department

College of Charleston

Charleston, SC USA

laughlina@g.cofc.edu

***Abstract – Ten sources to aid in our understanding and production of software for an activity tracker***

1. THE ARTICLES

[1] In this article, the authors focused in on two major issues with activity trackers; reverse engineering the communication protocols and hacking into the hardware itself. They quickly discovered vulnerabilities that were previously not understood. They were able to insert fake activity logs into another user’s device remotely. They were also able to attach a debugging tool to reveal specifics of the tracker that allowed them to discover the encryption key for the latest firmware versions that allowed them to decrypt any and all of the data that passed through the device. The authors agree that this paper should help reveal further issues with activity trackers as they proliferate throughout our culture.

[2] In this article the authors focus on the anonymization techniques used within the activity trackers. FitBit specifically has a social network of anonymized user data to communicate with others and provide extrinsic motivation. This article focuses on the analysis of the de-anonymization techniques that are being used to decrypt user’s data. The authors were able to simulate three different de-anonymization algorithms and quickly discovered they were able to achieve a rather in-depth activity log using the simulated techniques. This is obviously problematic for the user, as one’s privacy goes out the proverbial window if anyone on the internet can track your activity levels. This could be leveraged in a multitude of different ways including but not limited to: personal attacks, home invasions, security breaches, and more.

[3] In this article the authors focus in on the sharing aspect of activity trackers. Many insurance companies offer discounts for maintaining an active lifestyle. Companies too have offered incentives for sharing one’s intimate data. Activity trackers may even decide your fate in a court of law. Given the importance we put on these trackers, the integrity and accuracy of this data must be ensured. They authors quickly found that the traffic between Fitbit’s website and the base station was entirely unencrypted and they were able to upload modified data to the website. They found a similar security flaw in Garmin’s website. This kind of flaw is entirely unacceptable. Imagine going to court for a crime you didn’t commit and then being found guilty based on false information injected into your activity logs.

[4] In this article, the author focuses on one of the more intimate details your activity tracker may be publishing online without your consent. Approximately 200 users had their sexual activity published on the Fitbit website. This is obviously an issue, as virtually no one willingly shares when and for how long they have recently copulated. To limit this, Fitbit hid all activity records hosted on their site regardless of privacy settings. Despite this, many users had already taken screenshots and now possess a stranger’s sexual activity logs. Unless your fetish is digital exhibitionism, then you’re probably pretty upset by this. This type of failure costs Fitbit an incredible amount of money in lost assets, users, and general trust from the public.

[5] This article focuses on the communication channel in between one’s wearable device, and typically a mobile phone. This transfer of data leaves the user susceptible to a “man-in-the-middle” attack. These wearable devices also make authentication of a user difficult. Malicious hackers were able to inject data, hijack accounts, and even manipulate health data on the user’s profile. This was all possible because of the Bluetooth Low Energy technology that the activity tracker utilizes. Handing over the intimate details of one’s activity, location, and even sleep patterns is not advisable and leaves the user in an incredibly vulnerable situation. These privacy leaks are a great reason to further one’s understanding of cyber security before adopting new technologies.

Article [6] provides an interesting legal precedence on how data may be stored for a fitness tracker. The author dicusses a court case involving a violation of the fourth amendment due to a suspect having their fitbit searched during the investigation. Our software certainly should keep in mind what kind of data to report due to more than just one person being able to view the data. Too many features on our fitness tracker software would make any fitness tracker with our software installed on appear to be a cellular device which holds different legal standings. The scope certianly should be kept in mind when developing our activity tracker software.

Article [7] provides detailed information about the reliability and validity of fitness trackers on two different age groups. Reliability on our software is certainly a key aspect of our activity tracker software (especially in FURPS). An older demographic needs to be able to navigate the interface we develop for the actiity tracker software. While at the same time all age groups using our software need to be able to have access to potential advanced settings and simple settings such as text size and data poll rate. The software’s accuracy with the hardware of any fitness tracker is also essential in making sure all customers can reliabily trust the interpreted data.

Article [8] provides inforamtion on surveys of the importance on usability vs cost. Users had a significiant statistical reporting of a bigger interface icons than the low costs of the device. Results interpret as users caring more about appearance as a functional requirement than cost which is known as availbility in FURPS. Our software was most likely not going to emphasis the aesthetics of the interface and more on compatibility to reduce costs. However now with this article, our priorities have swinged.

Article [9] focuses on the usability of a reliable fitness tracker, including its software. The associates using the fitness tracker found excellent usability through improved physical behavior. Behaviors including sitting times, walking times, and organization scheduling times based on convenience of using an activity tracker. The emphasis is to make sure the software associated with the device installed on is easily available through decent performance, taking minimal amount of time to access any feature of the activity tracker.

Article [10] presents a health research team who had 8 months to design and discuss the theoretical approaches of Smart Walk. Smart Walk, a generic gitbit software, was designed for impoverished women with diseases that stopped their physical movement. After the 8th month, the research group determined that the health of the women studied on became very physically active. The research presented shows their activity tracker data displayed in a UI while describing their design process. The information given will come in handy with designing use cases and establish goals to reach towards as our software continues being developed.

Citations:

[1] Hossein Fereidooni-Jiska Classen-Tom Spink-Paul Patras-Ahmad-Reza Markus Miettinen-Matthias Hollick-Mauro Conti (2018). BREAKING FITNESS RECORDS WITHOUT MOVING: REVERSE ENGINEERING AND SPOOFING FITBIT - <https://link.springer.com/chapter/10.1007/978-3-319-66332-6_3>

[2] Rieck, J. (2016). Attacks on Fitness Trackers Revisited: A Case-Study of Unfit Firmware Security. Retrieved from <https://arxiv.org/pdf/1604.03313.pdf>

[3] Hill, K. (2011, August 11). Fitbit Moves Quickly After Users' Sex Stats Exposed. Retrieved from <https://www.forbes.com/sites/kashmirhill/2011/07/05/fitbit-moves-quickly-after-users-sex-stats-exposed/#4b6fecf4327a>

[4] Ching, K. W. (2016, May). Wearable Technology Devices Security and Privacy Vulnerability Analysis. Retrieved from https://pdfs.semanticscholar.org/ed59/579757a718715ef61c3346a667257464d312.pdf

[5] . Jian Mao-Wenqian Tian-Jingbo Jiang-Zhihong Zhou-Jianwei Liu (2018) Understanding Structure-based Social Network De-anonymization Techniques Via Empirical Analysis - <https://link.springer.com/article/10.1186/s13638-018-1291-2>

[6] Kendall, W. (2019). “Outrunning” the Fourth Amendment: A Functional Approach to Searches of Wearable Fitness Tracking Devices. *Southern Illinois University Law Journal*, *43*(2), 333–360. Retrieved from <http://search.ebscohost.com.nuncio.cofc.edu/login.aspx?direct=true&db=lft&AN=136723844&site=eds-live&scope=site>

[7] Burton, E., Hill, K. D., Lautenschlager, N. T., Thøgersen-Ntoumani, C., Lewin, G., Boyle, E., & Howie, E. (2018). Reliability and validity of two fitness tracker devices in the laboratory and home environment for older community-dwelling people. *BMC Geriatrics*, *18*(1), 103. <https://doi-org.nuncio.cofc.edu/10.1186/s12877-018-0793-4>

[8] Yuxi Jia, Wei Wang, Dong Wen, Lizhong Liang, Li Gao, & Jianbo Lei. (2018). Perceived user preferences and usability evaluation of mainstream wearable devices for health monitoring. *PeerJ*, 1. Retrieved from <http://search.ebscohost.com.nuncio.cofc.edu/login.aspx?direct=true&db=edb&AN=136234369&site=eds-live&scope=site>

[9] Brakenridge, C. L., Fjeldsoe, B. S., Young, D. C., Winkler, E. A. H., Dunstan, D. W., Straker, L. M., & Healy, G. N. (2016). Evaluating the effectiveness of organisational-level strategies with or without an activity tracker to reduce office workers’ sitting time: a cluster-randomised trial. *International Journal of Behavioral Nutrition & Physical Activity*, 13, 1–15. <https://doi-org.nuncio.cofc.edu/10.1186/s12966-016-0441-3>

[10] Joseph, R. P., Ainsworth, B. E., Vega-López, S., Adams, M. A., Hollingshead, K., Hooker, S. P., … Keller, C. (2019). Rationale and design of Smart Walk: A randomized controlled pilot trial of a smartphone-delivered physical activity and cardiometabolic risk reduction intervention for African American women. *Contemporary Clinical Trials*, 77, 46–60. <https://doi-org.nuncio.cofc.edu/10.1016/j.cct.2018.12.011>