POSTER

Citation for published version:
Krämer, M, Aspinall, D & Wolters, M 2016, POSTER: Weighing in eHealth Security. in CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 1832-1834, 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24/10/16. https://doi.org/10.1145/2976749.2989044

Digital Object Identifier (DOI):
10.1145/2976749.2989044

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
CCS '16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security

POSTER: Weighing in eHealth Security

A Security and Privacy Study of Smart Scales

Martin Krämer
University of Edinburgh, UK
info@martin-kraemer.net

David Aspinall
University of Edinburgh, UK
david.aspinall@ed.ac.uk

Maria Wolters
University of Edinburgh, UK
maria.wolters@ed.ac.uk

ABSTRACT

eHealth devices such as smart scales and wearable fitness trackers are a key part of many health technology solutions. However, these eHealth devices can be vulnerable to privacy and security related attacks. In this poster, we propose a security analysis framework for eHealth devices, called *mH-PriSe*, that will yield useful information for security analysts, vendors, health care providers, and consumers. We demonstrate our framework by analysing scales from 6 vendors. Our results show that while vendors strive to address security and privacy issues correctly, challenges remain in many cases. Only 5 out of 8 solutions can be recommended with some caveats whereas the remaining 3 solutions expose severe vulnerabilities.

Keywords

Wireless & mobile security, Internet-of-Things, eHealth

1. INTRODUCTION

Guaranteed security standards and unrestricted privacy protection are indispensable for data that are provided by fitness and health devices, such as smart scales and wearable trackers. While most consumer devices are mainly used by individuals for tracking their own health, data can be used in consultations with health care professionals or as evidence in courtrooms [19]. Consumer devices typically do not adhere to strict medical device standards [2] and may exhibit vulnerabilities not found in systems that are subject to privacy standards such as HIPAA [12, 10]. With *mH-PriSe* we propose a framework for the analysis of privacy and security aspects of eHealth solutions. We include static analysis, dynamic analysis and penetration testing functionality. With the various potential applications in mind we design this framework to be scalable and adjustable to the needs of security analysts. We validate this framework by investigating 8 different smart scales from 6 vendors. To the best of our knowledge, we are the first to provide a comparative analysis of privacy and security vulnerabilities of smart scales.

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.

DOI: http://dx.doi.org/10.1145/2976749.2989044

2. SMART SCALES IN EHEALTH

Here, we use eHealth loosely to describe practices designed to promote a person's health and well-being through technology. The kind of eHealth solutions we are interested in typically involve a sensor device (scale, activity tracker, blood oximeter etc.), a mobile application that is installed as a companion on the user's phone and a vendor-supplied web offering (c.f. Figure 1). Commonly other third party services (data analysis, advertising, social media) can be connected. The protocols employed are mostly standard, such as Bluetooth LE or Wifi for the device radios, and use HTTP(S) for data transfer. Since most solutions only support Android and iOS as mobile operating systems, we focus on those ecosystems here, and the static analysis part of the framework will be limited to Android only.

The study at hand focusses on Smart Scales as sensor devices. With Withings launching its first scale in 2012 the market by now has become very diverse. In a range from simple to advanced solutions these scales collect information on weight, Body Mass Index and body fat to water percentage, muscle mass and bone mass. The common idea is to track one's weight and further data on a daily basis to provide insights into health and well-being.

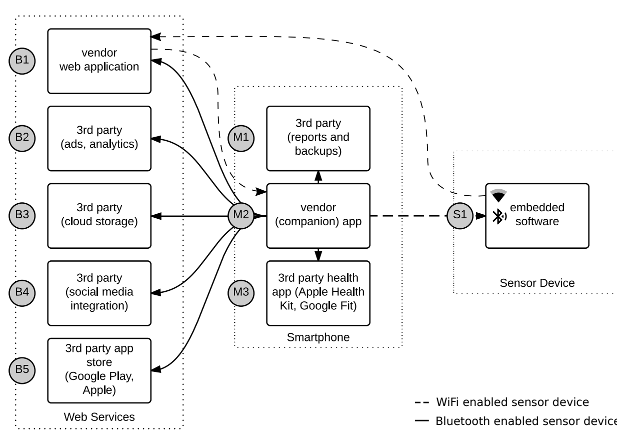

Figure 1: eHealth logical architecture

3. *mH-PriSe* ANALYSIS FRAMEWORK

Our analysis framework, *mH-PriSe*, and experiment setup allows for sound and methodological scientific research (c.f. Figure 2). We ran our experiments on a Lenovo X230 laptop with Kali Linux 2.0 and used an Atheros external WiFi card to create a hotspot. The test device was a rooted LG Nexus 5 with Android

6.0 installed. Test results were stored in a MySQL database and viewed through phpMyAdmin.

We have defined a threat model which includes assets, agents,

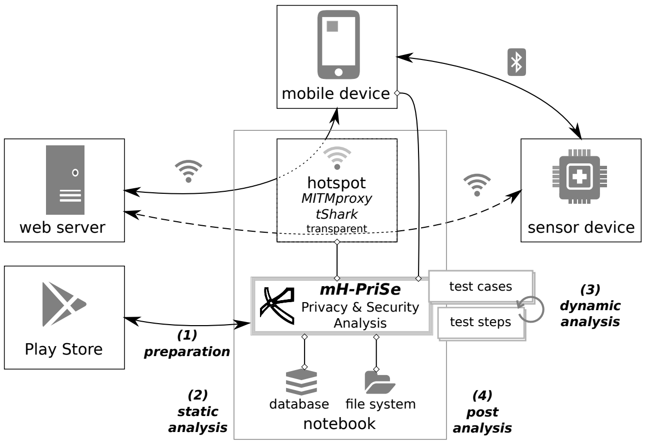

Figure 2: mHealth security and privacy analysis framework

weaknesses and attack vectors (full details in [16]). The *mH-PriSe* framework builds on this threat model and is defined by test cases (following attack vectors) and test steps (weaknesses) assigned to them. The view is complemented through the recording of informational steps. We investigated the actual behaviour of each solution in four steps. Preparatory functionality, which is summarized under the first step, is omitted here:

static analysis In 7 steps, we apply static analysis to development artefacts. Among others research tools used include *Androguard with Mallordoid,Drozer*, and Android SDK tools.

dynamic analysis Running 5 test cases and 44 test steps in total, we check for known weaknesses and search for issues. For this purpose MITMproxy is used to forge certificates and intercept any traffic on our hotspot.

post analysis Data collected through experimentation undergoes a rigorous, manual analysis. SSLLabs was used to analyze web server security. We also visualize the communication on a world map.

Subsequently the actual behaviour was compared to information retrieved from documented sources such as privacy policies and websites. Privacy policies are analysed according to their compliance with OECD guidelines [9] and EU regulations [7, 6].

4. RESULTS AND EVALUATION

We report our results under 8 main properties (rows) with a fail caused by major issues, warnings due to some issues and a pass based on some caveats (see Table 1). The first two rows of the table include findings related to data transmission between app and server or sensor and server. Weaknesses that have been identified in this context are highly severe. For example solutions Activ8rlives, HAPI, Thomson and iChoice failed to correctly use cryptography in their apps, including cases of missing traffic encryption, badly implemented SSL, un-salted passwords and re-constructable message authentication codes. The scales WS-30 and WS-50 by Withings as well as Aria by Fitbit connect directly to the internet and fail to make use of SSL encryption. The newer Body Cardio by Withings is the only scale in our test set that employs traffic encryption. These weaknesses allow for sessions stealing, traffic injection and tampering with measurements as indicated in Table 1.

The Fitbit Aria protocol, for example, is in version 39. After previous research had revealed issues, fixes have been applied [8, 18]. Our findings show that the protocol is still vulnerable to recomputing the MAC. What is even worse – if no precautions are taken – is that the scale reveals WiFi credentials during the pairing with a users home WiFi network.

The Thomson TBS705 scale and their mobile application show serious privacy weaknesses. Sending device tracking data to a Chinese advertising server and transferring unencrypted measurement data to a Europe server while offering no control over the data or providing a privacy policy, the solution violates many privacy principles found in the OECD guidelines.

While no solution looked intentionally malicious, many require updates to their mobile applications or sensor firmwares. Though solutions Withings Body Cardio and iChoice with SwissMed app are of commendable security standard, the latter performs slightly better with respect to privacy aspects. For the privacy we refer to the amount of data synchronised to different destinations and also aspects mentioned in privacy policies as compared to their actual behaviour.

Through our rigorous analysis we have identified the following main issues with smart scale solutions.

- ISS 1 *missing or broken encryption* – over the (wireless) network including app-to-server and sensor-to-server communication
- ISS 2 *improper certificate validation* – trust manager issues or invalid certificate
- ISS 3 *missing tampering protection* – traffic and messages are not protected against tampering
- ISS 4 *personal data leaked* – unnoticed data leakage; requires patches by vendors, mainly, to adhere to common practices in implementation
- ISS 5 *improper cryptography usage* – inadequate usage of cryptographic functions such as missing salts for hashes or MAC failures
- ISS 6 *weak password policies* – missing or weak password policies
- ISS 7 *account deletion* – flawed account deactivation or deletion processes
- ISS 8 *overprivileged application* – overprivileged applications installed on device

5. RELATED WORK

This study extends the previous work of Knorr et. al. [14, 15] to include sensor devices. Mense et al. provide more detail on the behaviour of mHealth applications with respect to privacy and the data being transmitted [17]. Baig et al. recently explored the research area of mHealth applications by reviewing their system design and the identified challenges and issues. Among those the biggest are security, privacy and safety [1].

Other researchers investigated single solutions more comprehensively to find similar security and privacy issues in many [5, 11]. Privacy and security issues in update mechanisms of sensor software and with mobile apps are detected in the work of Cyr et al. Various kinds of attacks on fitness devices have become popular in research (representative list): Over-the-air-attacks on fitness and health devices showing similar issues [11, 3] or reverse engineering of firmware and protocols [20, 4]. The closest work is Clausing et al. and Hilts et al. on a set of different activity trackers [13, 3].

	Activ8rLives	Fitbit Aria	HAPI Connected Scale	iChoice iChoice app	iChoice Medm app	Thomson TBS705	Withings WS-30 & WS-50	Withings Body Cardio
app to server	✗ trust issues; traffic tampering	✓ standard SSL	✗ no SSL; poor crypto usage	✗ trust issues;	✓ strong SSL	✗ no SSL; poor crypto usage	✓ standard SSL	
sensor to server	N/A	✗ no SSL; protocol reversed	N/A	N/A		N/A	✗ no SSL	✓ SSL
app & mobile device	✗ data leakage; no password policy; overprivileged	⚠ modern analytics library	✗ no encryption; broken crypto for passwords; no data wipe; *highly* overpriviledged	⚠ pwd chang policy and data wipe		✗ overpriviledged;data leakage; logging leakage; leaks credentials; no data wipe	⚠ modern analytics; no password change policy; reasonably priviledged	
sensor security	⚠ no strict BT pairing; no firmware update process	✗ leaks wifi credentials; unencrypted traffic; protocol reversed	⚠ no strict BT pairing; no firmware update process	⚠ no strict BT pairing; no firmware update process		⚠ no strict BT pairing; no firmware update process	✗ leaks session; no SSL	✓ safe pairing with SSL
web server	✗ broken account deletion process; weak password policy; vulnerable SSL config	✓ no password change policy; fine grained privacy settings	⚠ input not validated; no wipe option; password (change) polciy can be improved	✓ weak pwd policy; good privacy	⚠ same but SSL dated;	undetermined *not available*	✓ no password change policy; password policy can be improved	
data leakage	✗ data leaked; overprivileged app puts risk on updates	⚠ analytics data tracking; wlan ssid send	⚠ analytics tracking	✓ minimal data exchange and no leakage		✗ no data control; leaks device identifier	⚠ approx. location shared with vendor; modern analytics	
data storage according to privacy policy	UK ✓Europe	United States ✓United States, Safe-Harbor	Canada ✗none mentioned	United States ✓United States		Europe ✗no policy available	Europe ✓Europe	

Table 1: Security and privacy analysis results. Fail: major problems. Warn: some problems. Pass: with caveats

6. CONCLUSION

Our results show clear security and privacy problems in popular smart scale solutions. Vendors should be encouraged to meet security standards as defined for example by OWASP, CERT or others even for devices that are targeted at consumers. Flawed pairing processes and insecure software development lead to vulnerable solutions allowing attackers to easily eavesdrop on communication. In future work, we plan to create summaries of our findings that can be used by consumers and health care providers to take informed decisions when buying products or using data provided by products. We also plan to reach out to manufacturers to discuss our findings.

7. REFERENCES

[1] M. M. Baig, H. GholamHosseini, and M. J. Connolly. Mobile healthcare applications: system design review, critical issues and challenges. *Australasian physical & engineering sciences in medicine*, 38(1):23–38, 2015.

[2] F. Censi, E. Mattei, M. Triventi, and G. Calcagnini. Regulatory frameworks for mobile medical applications. *Expert Review of Medical Devices*, 12(3):273–278, may 2015.

[3] D.-I. E. Clausing, M. Schiefer, U. Lösche, and D.-I. M. Morgenstern. Security Evaluation of nine Fitness Trackers. Technical report, AV Test, 2015.

[4] M. Coppola. Hacking the Withings WS-30. https://poppopret.org/2013/06/10/summercon-2013-hacking-the-withings-ws-30/, 2013.

[5] B. Cyr, W. Horn, D. Miao, and M. Specter. Security Analysis of Wearable Fitness Devices (Fitbit). Technical report, Massachusetts Institute of Technology, 2014.

[6] European Comission. Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps. http://ec.europa.eu/digital-agenda/en/news/commission-staff-..., 2014.

[7] European Commission. Revisions of Medical Device Directives. https://ec.europa.eu/growth/sectors/medical-devices/regulatory-framework/revision/index_en.htm, 2015.

[8] M. Farrell. Fitbit without fitbit.com. https://github.com/micolous/helvetic/blob/master/protocol.md, 2014.

[9] H. Gassmann. OECD guidelines governing the protection of privacy and transborder flows of personal data. *Computer Networks (1976)*, 5(2):127–141, 1981.

[10] T. Glenn and S. Monteith. Privacy in the digital world: medical and health data outside of HIPAA protections. *Current psychiatry reports*, 16(11):494, nov 2014.

[11] R. Goyal, N. Dragoni, and A. Spognardi. Mind The Tracker You Wear - A Security Analysis of Wearable Health Trackers. In *SAC '16 Proceedings of the 31st Annual ACM Symposium on Applied Computing*, pages 131–136, 2016.

[12] A. M. Helm and D. Georgatos. Privacy and mHealth: How Mobile Health 'Apps' Fit into a Privacy Framework Not Limited to HIPAA. *Syracuse Law Review*, 64, may 2014.

[13] A. Hilts, C. Parsons, and J. Knockel. Every Step You Fake. Technical report, Open Effect Report, 2016.

[14] K. Knorr and D. Aspinall. Security testing for Android mHealth apps. In *Software Testing, Verification and Validation Workshops (ICSTW), 2015 IEEE Eighth International Conference on*, pages 1–8. IEEE, 2015.

[15] K. Knorr, D. Aspinall, and M. Wolters. *On the privacy, security and safety of blood pressure and diabetes apps*, volume 455, pages 571–584. Springer International Publishing, Cham, 2015.

[16] M. Krämer. *Health Monitors Under The Magnifying Glass: A Privacy And Security Study*. Master thesis, University of Edinburgh, 2016.

[17] A. Mense, S. Steger, M. Sulek, and D. Jukic. Analyzing Privacy Risks of mHealth Applications. In *Volume 221: Transforming Healthcare with the Internet of Things*, pages 41–45. IOS Press, 2016.

[18] K. Munro. Extracting your WPA PSK from bathroom scales. https://www.pentestpartners.com/blog/extracting-your-wpa-psk-from-bathroom-scales/, 2015.

[19] P. Olson. Fitbit Data Now Being Used In The Courtroom. http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#71a82d4209f8, 2014.

[20] J. Rieck. Attacks on Fitness Trackers Revisited: A Case-Study of Unfit Firmware Security. *CoRR*, 1604.03313:33–44, 2016.