Citation for published version:

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

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.
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.

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, 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 Mallordroid, 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].

### 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].
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


