Poster: A Set of Privacy Preserving Requirements For Smart Home Control System Mobile Apps

Sophia Hannah, Jonathan Ganz, Andy Applebaum, Matt Bishop and Karl Levitt
Department of Computer Science
University of California, Davis
Davis, California 95616
{shannah, jmganz, applebau, mabishop, knlevitt}@ucdavis.edu

***Abstract*—We propose a set of privacy preserving requirements based on our analysis of the AMX TPControl app for the Honda Smart Home. The Honda Smart Home contains controls and monitors designed to optimize energy use. Our study seeks to define privacy for the smart home app user, identify privacy requirements, while highlighting privacy vulnerabilities and ways to mitigate them. We focus on leaks that can lead to attacks against the smart home. To do this, we use argumentation, a logical formalism well-suited for balancing conflicting priorities and handling uncertainty, as a key component of our framework.**

***Keywords*—smart home, mobile application, privacy, leaks, security, threat model, argumentation.**

I. Introduction

One of the most salient challenges facing the deployment of new mobile apps is consumer concerns over privacy [2]. Within the smart home domain, energy use monitors and controllers compound existing mobile app privacy concerns due to the wide array of information they have access to. Not only do privacy violations leak information about the user, but they also leak information about the system itself, showing an attacker points of entry to damage the home.

We propose a set of privacy preserving requirements that can be used as part of future development and analysis of smart home apps. As a use case, we examine the Honda Smart Home (HSH), which was developed at the University of California, Davis campus to showcase energy efficient technologies, including a home energy management system (HEMS), distributed solar panels, and radiant geothermal heating and cooling. The HEMS monitors, controls, and optimizes electrical generation and consumption throughout the home's microgrid and has the ability to communicate with the grid to ensure that the smart home owner draws power at the most efficient times [5].

Within the HSH, the home owner can view historic and real-time energy consumption data using the AMX TPControl app. The AMX TPControl app communicates with several enabling technologies in the home, such as lighting control sensors, smart meters, temperature sensors, and smart appliances.

A. Motivation

The motivation for this work stems from our goal of identifying potential privacy leaks in the AMX TPControl app, an iOS app. At first, this amounted to "black-box testing" the app, allowing it to run unencumbered and using tools to measure its associated traffic. We used a man-in-the-middle proxy tool and Wireshark to perform initial analysis. This black-box testing approach is limited in determining the privacy leaks of the app. While Wireshark could intercept all plaintext communication, and MITM Proxy could expose HTTPS traffic, if the app uses encryption at the application layer as opposed to the network layer, we would be unable to identify what it was sending. With this limitation in mind, we realized the need for more fine-grained approaches such as dynamic taint analysis [3].

II. Previous Work

Previous studies have demonstrated privacy leaks associated with Android apps [3], and found that ad-libraries are a common cause of such leaks[4]. Outside of Android, iOS is also susceptible to such leaks. Morover, iOS faces vulnerabilities such as permission re-delegation and unauthorized access [1]. Leveraging insights from existing privacy leak studies can reveal commonalities among the platforms, such as the types of privacy-sensitive data accessed by the app.

Our study differs from previous work in this area in a number of ways. First, our threat model uses logical formalisms to examine confidentiality breaches that can lead to intrusions, considering the interaction of vulnerabilities such as permission re-delegation and remote code execution attacks. And, to our knowledge, this is the first study examining the privacy of a custom smart home controller app.

III. Formalizing Privacy Requirements

Balancing privacy requirements with usability is a challenging task due to the variability of the definition of privacy. Our goal is to provide a framework that identifies *critical* privacy concerns that can lead to intrusions and availability loss. We seek to accomplish this by logically encoding what it means for something to be private, ultimately constructing a knowledge base containing definitions for privacy as well as the consequences for violating those definitions.

Operationally, the challenge of our project takes on two forms: (1) balancing conflicting privacy definitions and requirements, and (2) determining whether or not a given app meets specified privacy goals. To address this, we use the logical formalism *argumentation*, explained below.

A. Argumentation

Computationally, argumentation is equivalent to non-monotonic logic: the goal is to accept a conclusion temporarily based on currently available evidence. In situations where evidence is contradictory, conclusions are made based on

acceptability semantics, which identify consistent lines of reasoning. With argumentation, the goal is not necessarily to determine what is *strictly* true, but rather what can be *reasonably concluded* to be true. This quality makes it well suited to privacy, where actions that apps take are obscured, individual policies can be contradictory, and consequences of privacy violations are unknown.

We apply argumentation logic as a way to reason about the consequences of privacy leaks and about the presence of leaks themselves. When reasoning about the presence of leaks, we acknowledge that the measurement of leaks is susceptible to uncertainty; network traffic analysis may indicate leaks, but it often does so unreliably. In analyzing consequences, if we do identify the leaks, it can be difficult to determine which exact consequences apply as leaks can produce multiple incompatible results. Argumentation can balance these conflicting results to produce a clear picture of how the leaks lead to future security vulnerabilities.

B. Defining Private and Sensitive Information

For purposes of this study, we are concerned with the privacy relating to apps for smart home management systems. We chose this specific area due to the serious ramifications that privacy leaks can cause – attacks on the home can result in real-world physical damage. We consider how privacy violations can be used to initiate attacks on the integrity and availability of the smart home energy system. We identify attacks against the home by examining the consequences of privacy leaks. These include, but are not limited to, the following:

- *Physical attacks* – information leaked can reveal whether or not a particular home is a viable target for burglary. Examples include leaking physical location (via GPS) along with knowledge that the user uses the AMX TPControl app (indicating the presence of valuable devices) or leaking energy usage that exposes whether anyone is present in the home.
- *Authentication attacks* – information leaked can reveal authentication credentials. This includes simple log-in information, such as the user credentials for the AMX TPControl app, and MAC addresses used for filtering.
- *Spoofing attacks* – similar to authentication attacks, these attacks identify information leaks that an attacker could exploit to masquerade as a legitimate user. As a simple example, an attacker could use knowledge of the local SSID to conduct a man-in-the-middle attack.
- *Takeover attacks* – these attacks have the most significant ramifications, wherein an attacker takes over local HEMS sensors and controllers. An example could be chaining authentication and spoofing attacks, posing as a user, and taking complete control over the home.

Our initial analysis highlighted several potential privacy concerns that could lead to future attacks. We found that the AMX TPControl app sent some data completely in the clear, revealing log-in information (the user's email address) to anyone monitoring the traffic. We also discovered that the app's ability to control the home was device-independent; the network did not perform any MAC address filtering, which could allow anyone with knowledge of the log-in credentials to control the home. Outside of this, the app was well designed, requesting no unnecessary permissions and featuring no ad integration, although it did send data to Apple's iCloud service.

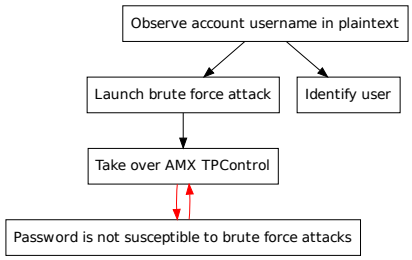

Fig. 1. Arguments from observing account username in plaintext

C. Future Work

We first plan on identifying privacy leaks typically not considered in the literature. As an example, local network information (e.g., MAC addresses, wireless BSSIDs and SSIDs, DHCP servers, gateways, etc.) is typically not considered sensitive, even though an attacker could use it to launch a remote strike; SSIDs could be used for spoofing attacks, MAC addresses could play into authentication, gateways can be targets for takeovers, etc. Our hope is to extend and integrate leak analysis tools from the literature into our framework so that we can monitor this type of information.

From there, we plan on extending our privacy model by introducing a logical language that relates privacy concepts to actionable consequences as well formalizing what an attacker can reasonably learn, infer, and act upon. Accompanying this language will be a knowledge base containing inference rules that, when seeded by observed and inferred privacy leaks, can be used to produce an argumentation framework exposing the routes an attacker can take to infiltrate the system. As a last step, we will produce an interface that can query an app, produce its leaks and consequences, and produce a set of mitigation techniques that developers can use to reduce the number of vulnerabilities.

References

[1] Y. Agarwal and M. Hall. Protectmyprivacy: Detecting and mitigating privacy leaks on ios devices using crowdsourcing. In *Proceeding of the 11th Annual International Conference on Mobile Systems, Applications, and Services*, MobiSys '13, pages 97–110, New York, NY, USA, 2013. ACM.

[2] J. L. Boyles, A. Smith, and M. Madden. Privacy and data management on mobile devices. *Pew Internet & American Life Project*, 2012.

[3] W. Enck, P. Gilbert, B. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth. Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones. In *Proc. of the USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, October 2010.

[4] C. Gibler, J. Crussell, J. Erickson, and H. Chen. Androidleaks: Automatically detecting potential privacy leaks in android applications on a large scale. In *Proceedings of the 5th International Conference on Trust and Trustworthy Computing*, TRUST'12, pages 291–307, Berlin, Heidelberg, 2012. Springer-Verlag.

[5] Honda. Honda Smart Home US. http://www.hondasmarthome.com/.