Security and the Internet of Things

**An Examination of Vulnerabilities in IoT Devices, With Guidelines to Protect the Consumer**

by: Richard Givens, CPSC 69700

Master’s Thesis for Master of Science in Computer Science

Instructor: Khaled Alzoubi, PhD

Lewis University, College of Arts and Sciences, Summer, 2019

Acknowledgements

Without the help of several persons within the Information Security Community, family, and friends research into this topic would meet with very little success. The author thanks the following people (either by name, name and handle, or handle where name is unknown):

**Family** particularly the author’s wife and children for persevering throughout several years of false starts, long nights of study, and for standing by the author during the challenges that life brings.

**Friends** some of whom must remain anonymous for reasons of either choice or professional necessity.

**Ben Actis (Ben-Ra)** for agreeing to examine the author’s project for any possible duplication of his previous work on an earlier generation Instant Pot Bluetooth device, and for sharing the resources, tools, and methods used in that project.

**Brenden Finegan(LordBeer)** for his continuing assistance in this and various other security research projects as a friend and partner in learning.

**Dr. Khaled Alzoubi** for expert guidance and advice, creating an environment that allows the creative freedom to explore topics of scientific interest.

**Dr. Ray Klump** for providing continuing guidance, advice, and opportunities to all students, and to the author on more than one occasion.

**Johnny Xmas** for being the first security researcher and member of the security community to answer certain questions and provide a level of detail to the author, when few were willing to take the time.

**Lesley Carhart (Hacks4Pancakes)** for convincing the author to return to Information Security after an initial failure several years ago, and for ongoing advice and guidance to all who are new to field.

**Marcus Perry** who, in his position as a member of the Lewis University staff assisting Veterans, showed extreme patience with the author many times over.

**Mark Carney (LargeCardinal)** for sharing his Pentesting Hardware – A Practical Handbook, a work in progress which he is freely available for all to use on GitHub, and for answering specific questions regarding the use of hardware and techniques in the testing of hardware and firmware on electronic devices.

**Roman Ortega Jr.** who, in his position as a member of the Lewis University staff assisting Veterans, provided an example of character that the author strived to achieve.

**The Chicago Burbsec Community, particularly PhreakingGeek and HackrDefendr** friends who have at various times provided insight, direction, advice and assistance in many projects and efforts over the course of a few years.

**Others within the Information Security Community** There are many within the Information Security Community that have offered advice or provided some content, instruction, or words of encouragement. Though far too many to name, every one of them is an invaluable member of this community. Thank you.

Abstract

This paper is an examination of vulnerabilities present in network attached home devices or appliances, commonly known as the Internet of Things (IoT) [2]. Various methods of attack are examined, along with demonstrations of specific attacks and vulnerabilities present in one or more devices. The Instant Pot WiFi 6 Quart Pressure Cooker [6,7], a household appliance available for purchase both online and in brick and mortar stores throughout North America and the United Kingdom is examined in depth. Finally, this paper will provide guidelines to consumers acquiring these devices, forming the base for informed purchasing guidelines and personal data/privacy protection to a segment of the population which may be neglected or uninformed.

Though these devices contain vulnerabilities common to many IoT devices, there is a possibility of previously undisclosed or unpublished vulnerabilities affecting either the manufacturer, or consumers. The author will follow industry standard responsible disclosure guidelines.

Several third parties have offered suggestions or mentioned casually how the device tested in this paper may be utilized as a physical weapon; these methods are not discussed out of an overabundance of caution, safety, and a moral obligation to prevent such knowledge from public discourse. The author strongly discourages such activity outside of a controlled environment with proper procedures, safeguards, and licensing, conducted only by professionals of appropriate authority and backgrounds.

## Table of Contents

## **Page**

## **List of Figures**

## The Instant Pot WiFi 6 Quart Pressure Cooker 10

## Instant Pot WiFi Control Board 11

## MM6411 WiFi Module 11

## SinoWealth SH79F64839 Processor 11

## Instant Pot WiFi in AP Mode 15

## Instant Pot Control App Requesting Location Access 17

## Instant Pot Control App Accepting Arbitrary User Input 19

## Instant Pot App Requesting Additional Permissions 19

## File Structure for the Instant Pot Control App Software 23

## Screenshot of Ghidra File Analysis Instant Pot .apk file 21

## Screenshot of Ghidra File Analysis on the libmsmart module 21

## File Structure for the Instant Pot plugins folder 23

## Code from the cordova-plugin-camera Module 24

## Code from the cordova-plugin-device Module 24

## Code from the FileReader.js File 25

## Code from the FileTranfer.js File 25

## Code from the LoadErrorDetector.js File 25

## Overview of the Android Phone filesystem and SLK Files 30

## **Page**

## The Instant Pot Facebook Open Community 31

## WHOIS Documentation for MAPP.APPSMB.COM 32

## Reply Email Regarding Privacy Inquiry From Instant Pot 33

## **Chapter 1: The Internet of Attack Vectors 1**

## Introduction 1

## Relevant Terms and Definitions 3

## Rise of the Machines 6

## Recent Events 7

## **Chapter 2: Testing Vulnerabilities in a Commercially Available Device 10**

## Device Information and Technical Specification 10

## The Privacy Policy 12

## Initial Testing and Results 15

## Examining the Control App 16

## Examining the Control App Code 20

## Examining the Midea Msmart IoT Platform 26

## Contacting the Vendor 29

## **Chapter 3: Guidelines for Consumers 30**

## The Legal Environment 31

## The Bitter Truth 32

## Determining Need Versus Novelty 34

## Understanding the Product 35

## **Page**

## Understanding the Environment 37

## **Chapter 4: Conclusions** **38**

## **References 43**

## **Appendix**

## A: Unformatted Log Sample from the SLK Folder 48

## B: Translation of the Midea IoT SDK Msmart Documentation 57

## C: Email to Instant Pot Privacy Office 74

Chapter 1. The Internet of Attack Vectors

* 1. Introduction

IoT refers to a collection of devices capable of communication via wireless or physical adapters, connecting them directly to the network of homes and businesses. This allows for near instantaneous communications between the device, command and control servers, users, administrators, mobile applications and web-based dashboards. Early IoT devices consisted of large appliances, such as refrigerators. In 2000, LG launched the Internet Digital DIOS Refrigerator for $15,000.00. The DIOS contained a modem, Ethernet port, LCD touchscreen, a camera, microphone, speakers, and external DVD ports and was as much of a computer as it was a kitchen appliance [12].

Since the launch of the LG DIOS, IoT has expanded to include many other devices in household and industrial applications. In the home baby monitors, televisions, digital picture frames, radios, light bulbs, coffee makers, air conditioners and thermostats comprise but a portion of the Internet connected devices consumers allow in their homes. Rather than following Moore’s Law of increased computing power and decreased cost [20] , these new computerized devices follow a new guideline: any device a consumer interacts with does now, or will in the future, contain network technology allowing it to send or receive signals via the Internet. This creates an environment of innovation as manufacturers scramble to meet consumer demand, creating new devices and new methods of interaction across the personal and household device landscape. Being able to control the temperature of one’s home, shop for necessities, and communicate with family from the comfort of a couch which provides charging for one’s smartphone is now the pinnacle of the consumer experience.

This scramble to bring goods to market first creates an environment in which the implications to privacy and data security become secondary or even tertiary concerns, resulting in negative impact to the personal data and privacy of consumers in an age where these issues are among the foremost in their minds.

The following section will define key terms and discuss several events involving IoT security which impact consumers. Next, this paper discusses the existence of one or more vulnerabilities existing in a commercially available IoT device, which impact the user’s privacy and/or security posture. Finally, this section will discuss action taken by the vendor, manufacturer, or distributor upon notification.

In the final section, the paper develops security guidelines for consumers for use in purchasing an IoT device. These guidelines will borrow heavily from the best practices of businesses and recommendations by governing authorities, presenting them in a concise manner which assumes nothing regarding the technical expertise, training, experience or education of the reader. Following this information, a consumer should have the necessary facts, information, and guidelines enabling an evaluation of the need, risk, and benefit of purchasing IoT devices in order to make an informed decision.

* 1. Relevant Terms and Definitions

Factors contributing, at least in part, to the frustration and confusion of consumers regarding IoT security, indeed all security concerning information systems, data, and privacy, are the numerous technical terms and abbreviations which makes sense to those familiar with computing but seldom used outside these specific cases. This section attempts to define common terms used within the practice of information security in a concise manner, easily understood by readers of all technical or non-technical backgrounds. These definitions are not exhaustive; however, these terms will appear in several places throughout this publication, thus defining them in the beginning is both necessary and valuable to the reader. Other unique terms will occur once, defined at that time.

**Access Point(AP):** Also known as a **Wireless Access Point (WAP)**; this is an electronic device physically connected to a network router, switch or hub and projects a WiFi signal to a designated area [32]. Examples of Access Points include devices found in many businesses which advertise free WiFi for customers.

**Botnet:** A botnet is a network of computers operating in parallel, pooling resources to achieve predetermined goals. The common definition for a botnet is a collection of Internet connected devices which have been compromised by a malicious third party and utilized to launch attacks, such as in the case of the Mirai Botnet [10]. Though botnets with mundane purposes exist, consumers will most likely encounter those exhibiting malicious behavior.

**Denial of Service (DOS):** “A denial-of-service (DoS) attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor,” [4,18 ]. Common methods involve flooding a target computer or server with connection requests or responses to fake connection requests, overwhelming the target machine until it is eventually unable to initiate or respond to any subsequent request. A form of DoS attack, the **Distributed Denial of Service Attacks (DDoS)**, involves multiple computers simultaneously initiating attacks against a single target or a small group of targets. DDoS attacks require a level of coordination which is present in botnets.

**Evil Twin:** An Evil Twin is an Access Point created by a malicious third party which mimics a legitimate Access Point in general appearance, network name, channel, and electronic address, also known as the **Media Access Control (MAC) address**.An Evil Twin is designed to lure unsuspecting users to connect to it, thinking it is a legitimate AP, and then either harvest credentials such as usernames and passwords, or as platform from which the attacker launches other attacks. Some Evil Twins may present an account sign on page, requesting social media account credentials. It is possible that a user will never detect this attack, as the Evil Twin AP could pass legitimate traffic to the Internet once it has completed its task (while still monitoring traffic from the user and collecting as much as possible); in other cases, the Evil Twin will drop all traffic from the user and seemingly disconnect after completing its initial task. [33].

**Firmware:** Firmware is the operating system of an electronic device, permanently programmed into Read Only Memory (ROM). In most cases, the only access of firmware allowed to users is the ability to update it by a means called flashing. Examples of firmware include the operating systems of most mobile devices, printers, routers, and integrated electronic components of computers and computer peripherals.

**Man in the Middle (MITM):** Man in the middle attacks involve a third party inserting custom traffic in, or eavesdropping on network traffic between one or more devices, such as computer and a router or access point [31]. MITM attacks may be either active or passive. In an active MITM attack, the malicious third party engages in sending or altering traffic, while in the passive attack, the malicious third party observes and records traffic. The traffic observed is either encrypted, meaning that it is not readable by an outside party, or “in the clear”, which is plaintext characters easily decipherable.

**Patch:** A patch is a software or firmware modification which occurs post production to remediate an issue which was undetected or unresolved during the development and testing phases of the product or service, or to provide enhanced reliability, performance, or compatibility in the wake of a technological improvement or innovation. At times, a patch may include several modifications which both provide remediation and enhancement. **Patching** is the term associated with applying a patch and may occur at any time post production. Though the purpose of a patch is to improve a product, or remediate some unaddressed issue, it may at times introduce other flaws, particularly if the patch is developed hastily.

* 1. Rise of the Machines

In 1966, German Computer Scientist Karl Steinbuch is reported as saying “In a few decades time, computers will be interwoven into almost every industrial product,” [25]. This prediction has indeed come true, as computers or computing devices form the backbone of nearly every modern convenience, product, or service. The pace of innovation in computing is such that computers and computing devices have moved from the realm of enterprise business and government research to mainstream use by home users, small businesses, and classes in only 73 years. The ENIAC computer came into service in 1946 [5], after the end of World War Two; though an ever-decreasing number, there are still Veterans alive who fought in the battles of World War Two, and civilians who lived through those times. The entire existence of modern computers, from vacuum tubes to Quantum Computing is measured in less than a human lifetime. This rapid pace of development and deployment creates a unique set of problems in which the products sold to consumers are released before society and the legal system has time to catch up. While government regulation has largely kept pace with industrial standards since at least the turn of the 20th Century, regulators generally possess a great deal of uncertainty about the newest innovations in computing, creating a loop of inaction which stifles further creativity and adoption [5].

Of interest is the Internet of Things (IoT) and so called “smart homes” in which numerous Internet connected devices, many of them mundane household appliances, occupy space in the home’s network connected infrastructure, exchange

data, and communicate both within the local network and over areas of geographical distance via web and mobile applications. Many of these devices are “always on”, or constantly providing updates and communicating with various end points, whether a server or the homeowner’s phone. As stated by the National Institutes of Health through the National Center for Biotechnology Information: “Application of the IoT model to smart homes, by connecting objects to the Internet, poses new security and privacy challenges in terms of the confidentiality, authenticity, and integrity of the data sensed, collected, and exchanged by the IoT objects. These challenges make smart homes extremely vulnerable to different types of security attacks, resulting in IoT-based smart homes being insecure. Therefore, it is necessary to identify the possible security risks to develop a complete picture of the security status of smart homes,”[1].

* 1. Recent Events

Though a relatively young technology, IoT attacks continue to increase at an alarming rate. One contributing factor is the increase of adoption by consumers; the number of installed IoT devices is expected to increase five hundred percent from 2015 levels, reaching an estimated seventy-five billion devices [8]. Recent advances in communication technology, namely 5G wireless networks, may alter this prediction, resulting in an increase above forecasts. The rate and number of attacks affecting IoT devices will rise in direct proportion to the rate of adoption and deployment of these devices. All attacks follow the path of least resistance; a malicious third party will stop searching for a method to obtain their goal once they have identified the first available means matching their criteria.

In 2007, doctors treating former Vice President Dick Cheney disabled the WiFi connectivity of his implanted pacemaker amid fears that a malicious third party could access and gain control of the device, causing it to administer shocks or shut down completely [28]. Though there were several other implantable medical device vulnerabilities disclosed in the preceding and following years, in 2017 nearly half a million pacemakers manufactured by Abbott were the subject of a recall by the FDA amid demonstration that an attacker could use commercially available equipment to intercept wireless signals from pacemakers, and issue malicious commands causing serious injury or death [22].

In 2017 Burger King released a commercial that, as a marketing stunt, utilized keywords which activated Google Home devices in the homes of consumers, prompting the device to describe one of Burger King’s menu items [14]. Google responded by altering the Google Home devices in some manner, which prevented them from responding to the commercials. While not explicitly malicious, this action by Burger King is viewed by many as an unethical violation of privacy.

In 2018, a software update to the Tesla line of automobiles caused some models to experience performance issues and loss of power [11]. This software was delivered wireless to the Tesla automobiles, as part of an update to the Linux operating system powering all Tesla models [29]. As Linux is an open source operating system, one may expect to see other vulnerabilities surface, such as the March 2019 exploit which caused a Tesla vehicle on autopilot to switch lanes into oncoming traffic [9].

In 2016, security researchers found a flaw in the Android app controlling IoT devices manufactured by Belkin, which allowed anyone on the same network as the device gain access to the user’s cellphone to copy files and track the phone’s location, [24]. Additional research revealed a flaw enabling control of the IoT devices by a third party. Belkin has since patched these flaws, but until their discovery, they affected a wide range of devices, all managed under the same Android app.

It is unclear if these vulnerabilities ever reached the point of exploitation by malicious third parties. However, other vulnerabilities in commercial, medical, and industrial IoT devices exist while remaining unidentified. Both the pace of innovation and feasible scope of security research make it impossible to disclose all, if many, of the risks associated with these devices. Further research and a concerted effort of cooperation between the manufacturers of these devices and the researchers examining them, in tandem with robust product development and testing procedures can address some of the concerns, however.

Chapter 2. Testing Vulnerabilities in a Commercially Available Device

To discuss the threats and vulnerabilities inherit in IOT devices, it is necessary to go beyond the brief introduction of the previous section. To that end, this section will begin the examination of a commercially available device with no previously reported threats or vulnerabilities, the Instant Pot WiFi 6 Quart Pressure Cooker (Instant Pot WiFi), [6, 7], [Figure 1].



Figure : The Instant Pot Smart WiFi 6 Quart Pressure Cooker. Image from https://instantpot.com/portfolio-item/instant-pot-smart-wifi/

* 1. Device Information and Technical Specifications

The Instant Pot WiFi is a pressure cooker with a network interface, through which a user controls the cooker using an Android or iOS device [7]. The IoT heart of the device is the programmable control board, [Figure 2], with an integrated Midea MM6411 wireless network adapter, [Figure 3 ], and 32-bit SinoWealth ARM processor, model SH79F6483P [Figure 4]. Though markings on the processor identify the manufacturer and model, the website for SinoWealth contains no information on this module.



Figure Instant Pot WiFi Control Board



Figure The MM6411 WiFi Module

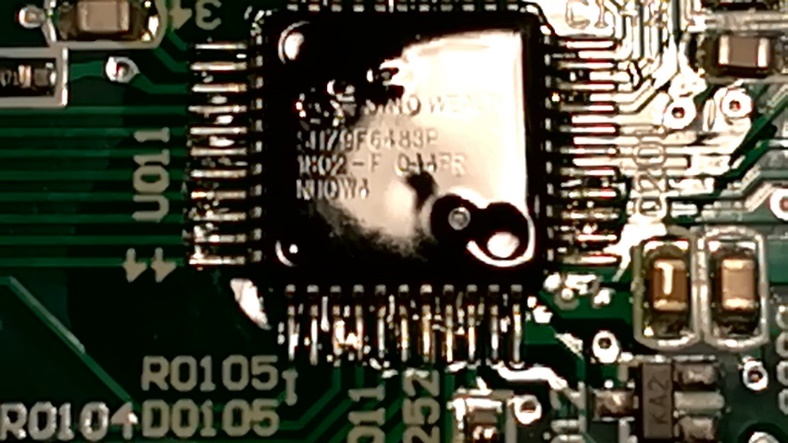


Figure The SinoWealth SH79F6483P Processor

The FCC Identifier, 2AIRV0004 [16], provides information on the manufacturer of the WiFi Module, Midea Smart Technology Co., LTD in the Nanshan District, Shenzhen, China (Midea Global). Midea Global is a relatively prolific and popular manufacturer or household appliances and smart devices throughout Asia, with several of their devices available commercially in Europe and North America [30]. In the United States they are relatively unknown, however the wireless network cards powering their IoT devices are also found in many other devices distributed by other companies. Like many global corporations, Midea Global consists of several smaller components focusing on specialized activities. One of these activities is an IoT cloud infrastructure: M\*Smart, which uses a unified software development kit [16], provided to distributers of IoT devices for usage monitoring [17]. More on M\*Smart will follow in later sections.

* 1. The Privacy Policy

Before discussing the research of the control app, it is necessary to review the privacy policy for the parent company of the Instant Pot WiFi, Instant Brands, Inc. This review will set the context for the following sections.

Through its full privacy policy [23], Instant Brands makes the following assertations:

“When you purchase an Instant Pot product, you may download an APP to help you get the full array of services offered by Instant Pot. With your express consent, the APP will collect your use data of the Instant Pot product.”

“This information is used to respond to your needs and interests as well as any support you may need.”

“Whether it was collected through the website, the online store or Instant Pot Services, Personal Data is never sold or disclosed without consent, except in the rare cases where it is required to do so by law.”

“However, in the course of business, Instant Pot may hire third party individuals or organizations to help deliver our services. Instant Pot may also hire third parties to operate, maintain, repair, or otherwise improve or preserve files or systems.”

“In those cases, the third parties only process Personal Data collected by Instant Pot, on Instant Pot’s behalf, under Instant Pot’s written instructions, and/or under contractual arrangements containing specific clauses that demand the same level of security and protection of the Personal Data shared with them as provided for by Instant Pot. All third parties engaged by Instant Pot are subject to this Privacy Policy and to compliance monitoring in that regard.”

“Instant Pot stores and processes your Personal Data in Canada and with AWS under the highest data security standards. AWS is certified under the EU-US Privacy Shield.”

The policy concludes with a statement providing an email address and title for whom to address concerns and questions regarding Instant Pot’s privacy policy.

* 1. Initial Testing and Results

Initial testing of the Instant Pot WiFi focused solely on easily identifiable and exploitable vulnerabilities which would require immediate disclosure, thus affecting the outcome of this research. This testing involved the use of remote protocols attempting to access the device without using the Android or iOS app, with the goal of gaining control of the underlying filesystem, or access to user credentials.

When the Instant Pot WiFi is powered on, it runs in a default AP mode, broadcasting its unique identifier publicly so that users of the device may be able to easily identify it and connect to it using the app [Figure 5]. One observable flaw is the lack of a unique password when connecting to the device. Per Instant Pot documentation, the default password for all Instant Pot WiFi devices is “12345678,” [7]. Also, the Instant Pot WiFi broadcasts an easily identifiable SSID: its MAC address prefixed by “Instant\_Pot\_, [26], note in Figure 5 that the Instant Pot identifies itself as “GD Midea Air Conditioning Equipment.”

Another observable, yet unavoidable flaw is the necessity of the Instant Pot WiFi to accept connections from any device using the SSID and password combination. The Instant Pot WiFi has no means of verifying the device or platform from which a connection request is sent, thus it must rely upon the supplied credentials. This allows a malicious user to connect to the device while it is in AP mode and send data to or receive it from the device across the connection. However it must be noted that all observed traffic to and from the device is encrypted and it would require considerable effort for an attacker to determine the content of any information sent or received. Finally, the Instant Pot WiFi remains in its AP mode for only thirty minutes. If during that period there is no successful pairing of the device to a network, then it will power down automatically and close all active connections.

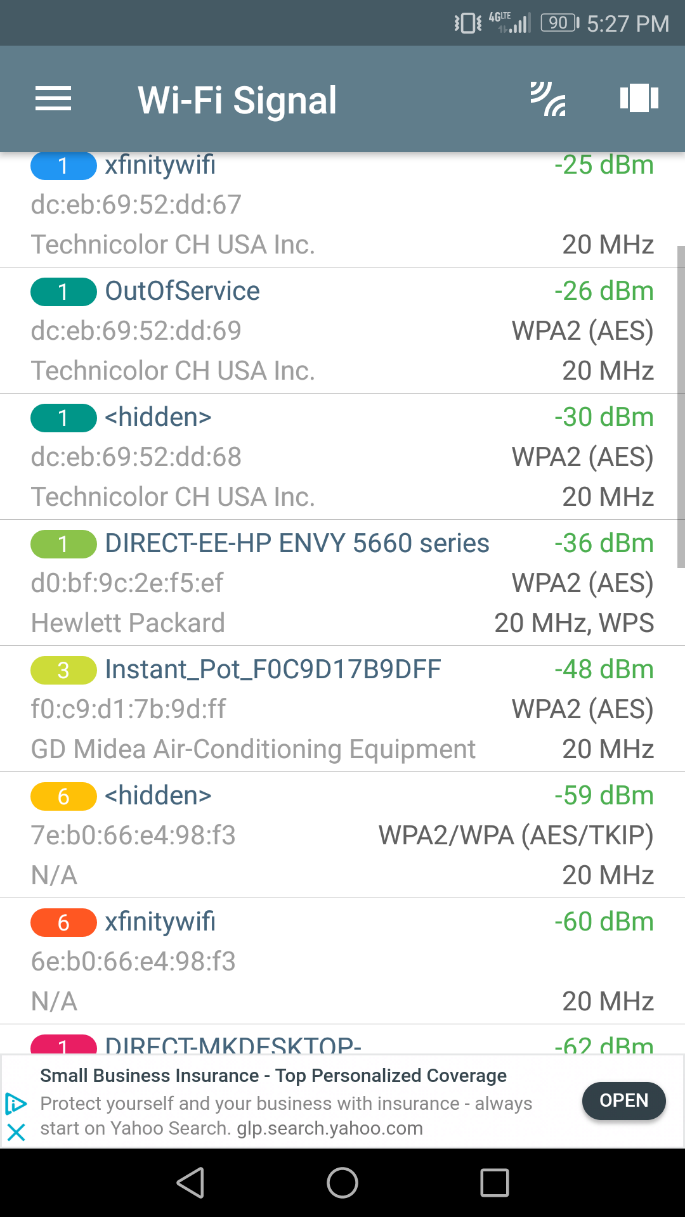


Figure Screenshot from and Android Phone Using Net Analyzer to identify the Instant Pot WiFi in its AP Mode

Though the Instant Pot WiFi will accept any connection, it is impossible to determine from that connection what the underlying filesystem, firmware, or operating system that controls the device is. The Instant Pot WiFi is resistant to port-scanning, reporting all ports closed, and will not respond to Secure Shell (SSH), File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), Telnet, or Remote Desktop requests from a third-party computer, which will only report standard “no-response” error messages.

Similarly, the method by which the Instant Pot WiFi stores network credentials is unknown. Repeated pairing of the device to a network is unnecessary, so it stores the credentials in some permanent memory location, but the credential exchange between the device and the network is encrypted, like traffic during the initial pairing.

Throughout this initial testing, it was determined that an attack on the device would have little impact on the user, beyond simple mischief. A malicious user could create a situation resulting in a DoS attack on the device itself but could not use these means to launch a DoS or DDoS attack against other devices, networks or computers, nor could they result in the recovery of network credentials without advanced decryption methods.

* 1. Examination of the Control App

While the Instant Pot WiFi is a networked device that sends and receives signals, it is a very simplistic device which serves the single purpose of preparing food. Other than storing the user’s network credentials, it does not appear to have any unexpected functionality or interaction with the user’s environment. The Android and iOS control app however, is a complex software application which contains additional functionality beyond the code necessary to control the device.

Testing of the Instant Pot Wifi control app utilized the most recent version available for Android devices on the Google Play Store.

Upon first opening the app, the user is present with a popup message on his or her screen, requesting permission for the app to access the device’s location [Figure 6].

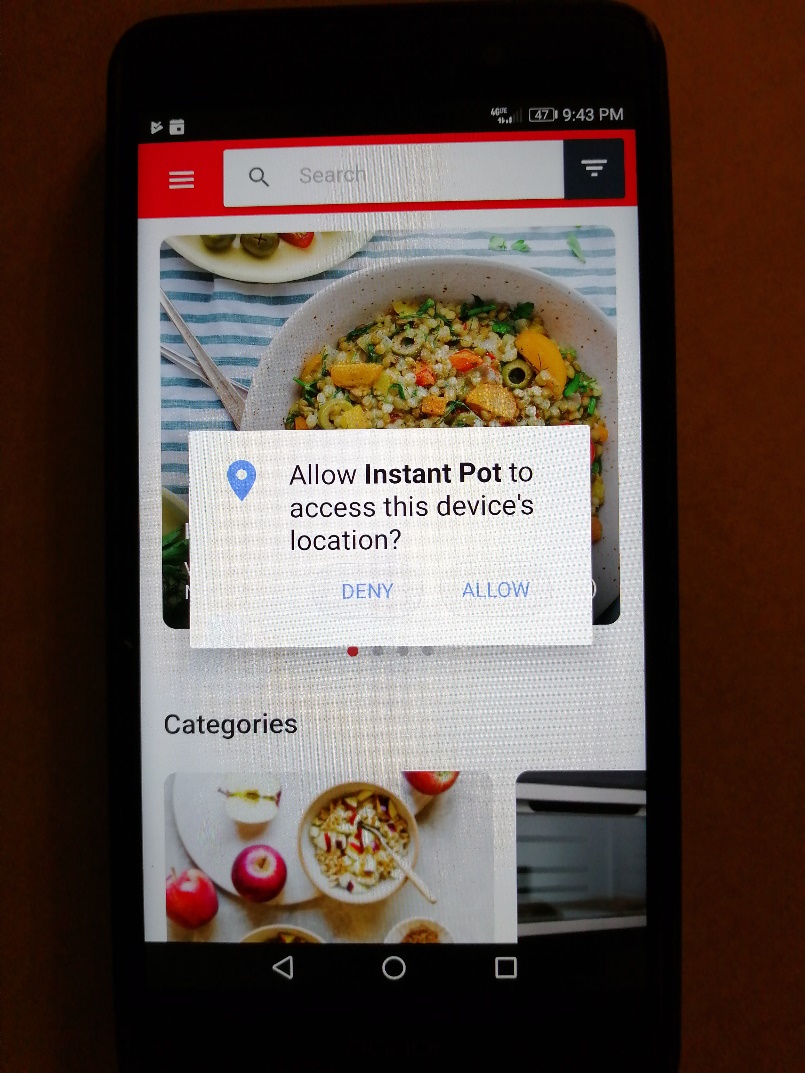


Figure Picture of Android phone with the Instant Pot control app enabled

Though there are numerous complaints on the app’s reviews section regarding this request, Instant Pot states such permission is a requirement of the Android OS in order to pair the Instant Pot WiFi with an Android device. This requirement was tested against a fresh install of the app on an Android phone; location access was denied, and the pairing process initiated. The Android phone successfully paired with the Instant Pot WiFi, despite the user denying location permissions to the app.

During the pairing process, if the user has not already created an account with Instant Pot, he or she is required to do so. The user creates a username, provides an email address, and composes a password. There are no authentication methods in place to verify a user once he or she signs up for an account. Rather than generate an email and wait on user supplied input or verification, the app accepts arbitrary strings of characters for the username, and will accept arbitrary strings for the email, providing the string is formatted to look like an email address, [Figure 7]. While not initially detrimental to the users of the Instant Pot WiFi, this does affect the company itself. By allowing arbitrary strings in the username fields of their accounts database, this may introduce vulnerabilities that could allow a malicious third party to access, alter, delete or add to the data in this database. However it is not possible to test this theory without the full knowledge, permission and cooperation of Instant Brands, Inc.

On any subsequent startup of the app, it once again asks for device permissions. However the requested permissions are different from the first location request, and relate to the device’s “photos, media, and files on your device,” [Figure 8]. The reason for these permission requests is unclear, as the app provides no functionality to add, save, or upload any files, photographs or other media. Users can create a “grocery list” of ingredients, or select a recipe as a favorite, but these functions do not require the user to add or download any file, media, or image. There is no discernible reason for the app to request these permissions.

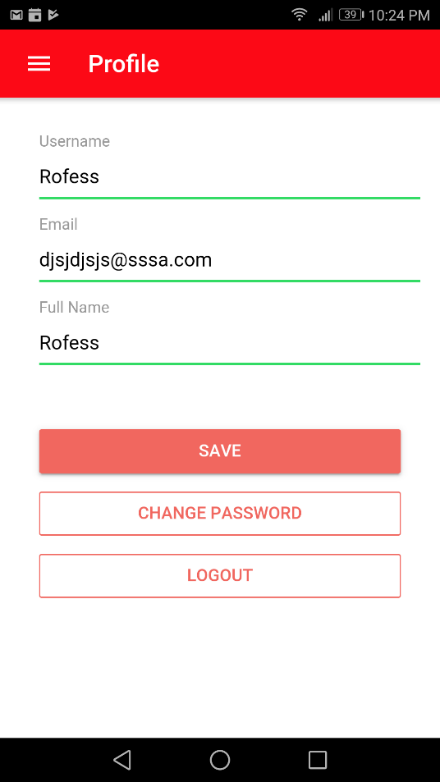


Figure Screenshot of the Instant Pot

Control App with Arbitrary User Input

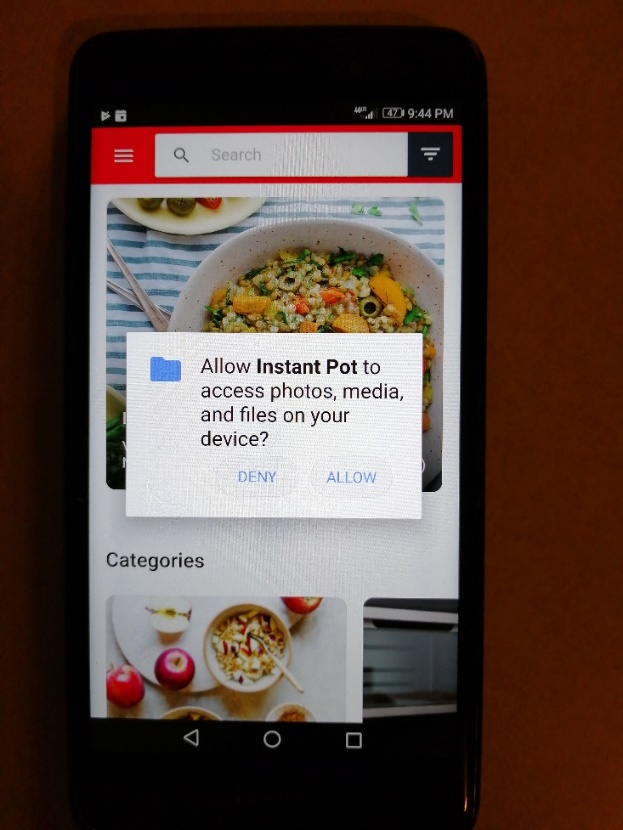


Figure Picture of Android Phone with the Instant Pot Control App Requesting Additional Unnecessary Permissions on a Subsequent Start

Further investigation of the app required the decompiling of the .apk file into its individual modules. This was accomplished by downloading the full .apk file from the Google Play Store, via the APK Download Chrome Extension. This allows a user to download the .apk file directly to a Windows PC or other device capable of using the Google Chrome Browser.

* 1. Examining the Control App Code

Using the freeware utility 7Zip, the contents of the .apk file were extracted into their individual modules, creating separate folders and files for each component, [Figure 9].

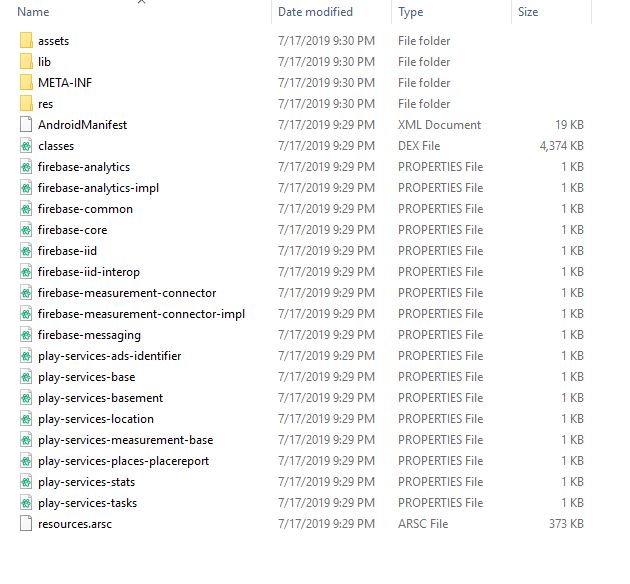


Figure File structure for the Instant Pot control app

The freeware reverse engineering tool Ghidra, created by the National Security Agency was used to analyze the lib folder and its subfolders: arm64-v8a, armabi-v7a, x86, and x86\_64. Each subfolder contained identically named files: libmsmart and libsqlc-native-driver, [Figure 10]. Each file is written in a version of Assembly language that corresponds to the subfolder name; the subfolder x86 contains two files written in x86 Assembly, for example, [Figure 11].

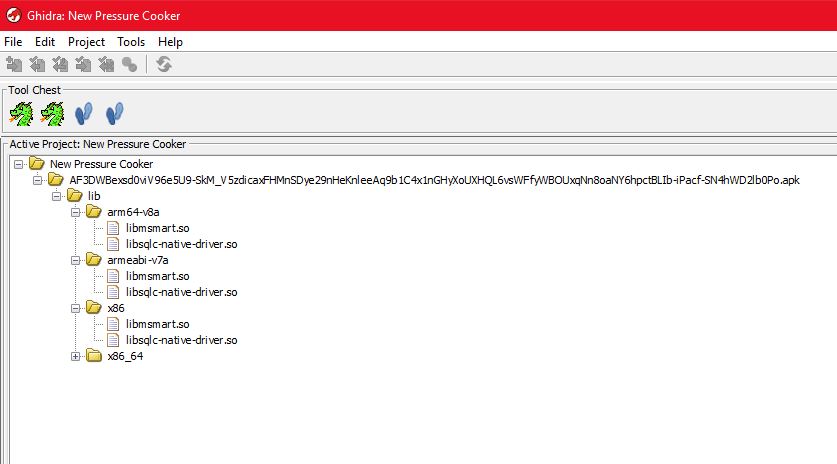


Figure Screenshot from Ghidra showing the analyzed files from the full Instant Pot Control .apk file

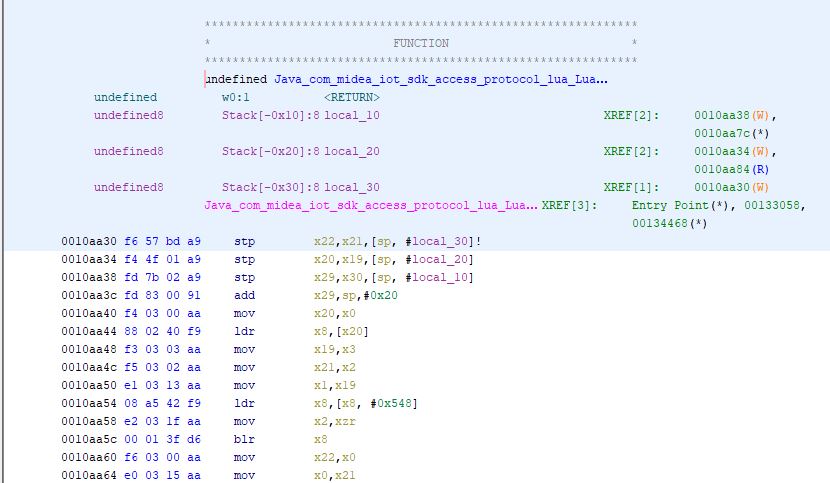


Figure Screenshot from Ghidra analysis of the libmsmart file

Both the filename for libmsmart and various lines in its code, an example in Figure 10 above, reveal that it is part of the Media Smart IOT SDK, [15].The exact functionality of this specific code is unclear, however subsequent sections will detail the capabilities of the SDK and its impact on user privacy.

Next, research moved to the assets/www subfolder; within are several more subfolders, including another assets subfolder. Of interest are the build subfolder, which contains the main app functionality, and the plugins subfolder, which contains multiple smaller modules which add to the functionality of the app.

The Instant Pot app uses the Apache Cordova open source mobile development framework [21], [Figure 12] and as such includes multiple JavaScript plugins. Among these plugins are wifiwizard2, which provides the pairing functionality, however several plugins stand out: cordova-plugin-camera, cordova-plugin-device, cordova-plugin-file, and cordova-plugin-file-transfer.

Examining the code for cordova-plugin-camera reveals that it is a module for taking pictures using the device camera retrieving images from the device’s image gallery [Figure 13]. Recalling that one of the permissions which the Instant Pot app requests is access to camera, files, and media it appears this module is active, yet there is no functionality in the Instant Pot app to create, download, or upload images [Figure 13].

The cordova-plugin-device module provides information on the user’s device, creating an object which contains the manufacturer, model, serial number, and UUID of the user’s phone [Figure 14].

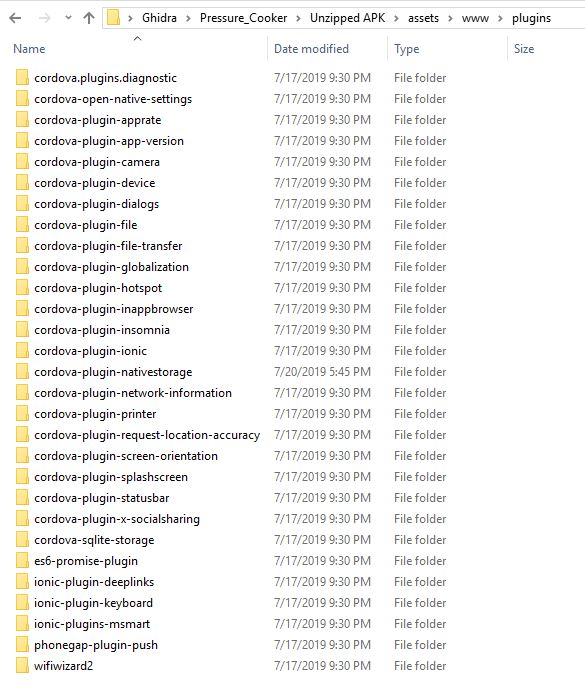


Figure File Structure of the Instant Pot control apps assets/www/plugins folder

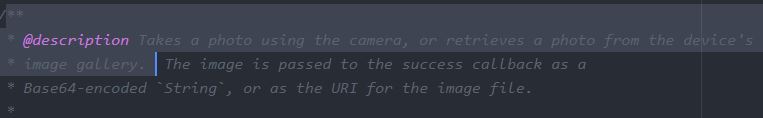


Figure Screenshot of code comments in the cordova-plugin-camera code, as viewed from the Atom text editor

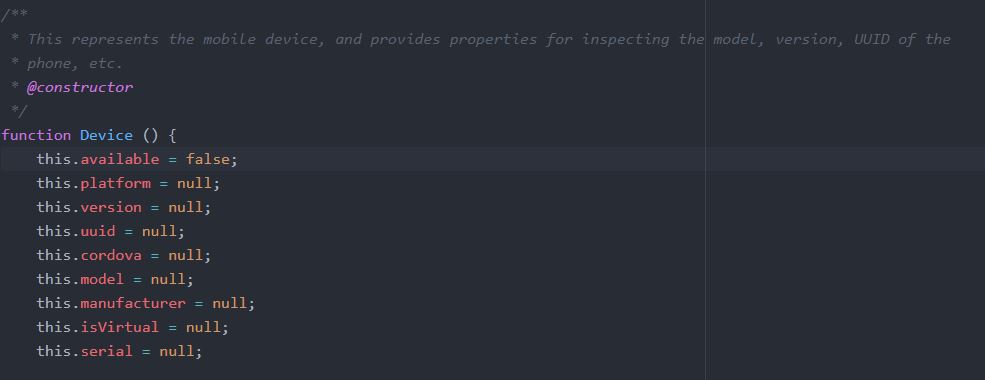


Figure Screenshot of code comments and Device function in the cordova-plugin-device module, as viewed from the Atom text editor

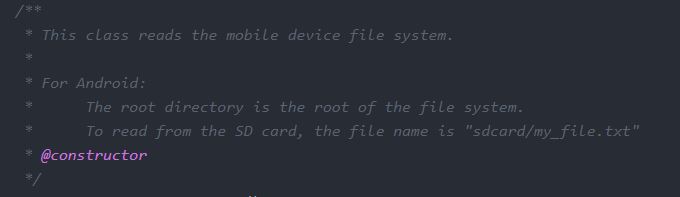
The cordova-plugin-file subfolder contains additional subfolders and JavaScript files. Of note is the FileReader.js file, [Figure 15], which reads the mobile device filesystem. Other .js files provide functionality for writing and uploading files and inspecting the directory of the mobile device, [Figure 16]. One plausible reason for this, and the cordova-plugin-device functionality is error reporting. Instant Pot uses Functional Software’s Sentry platform for automated error reporting, as determined by examining the assets/www/build folder containing the load-error-detector.js file, [Figure 17]. While this is a very plausible explanation for the existence of these plugins, the file transfer uses an unencrypted method, via the FileTransfer.js file which states in the code comments that it is using HTTP PUT and POST requests, rather than HTTPS.

Figure Screenshot of code comments in the FileReader.js file, as viewed from the Atom text editor

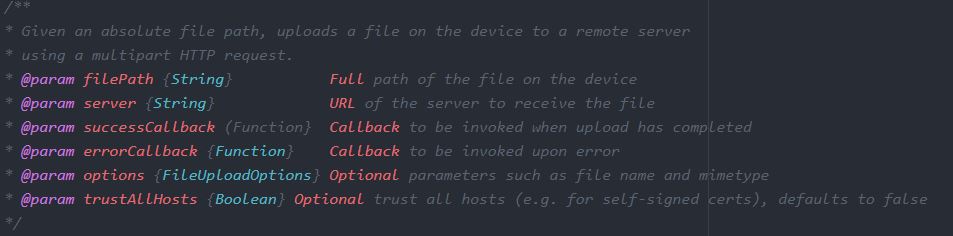


Figure of FileTransfer.js file

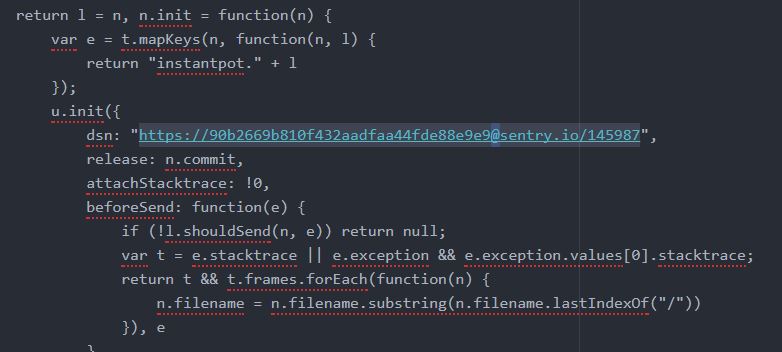


Figure Screenshot of the LoadErrorDetector code specifying the Sentry URL

* 1. Examining the Midea MSmart IoT Platform

In addition to cordova plugins, there are three ionic plugins; the ionic-plugins-msmart subfolder contains the MSmart.js file. When examined, this file contains a mix of English language characters for the main code, and code comments in what appear to be primarily Chinese. The “msmart” naming convention is consistent with earlier examination of the libmsmart file analyzed by Ghidra. It contains functionality to send device, network, and Instant Pot account information to a remote server, as well as relaying stop and start commands to the Instant Pot WiFi device.

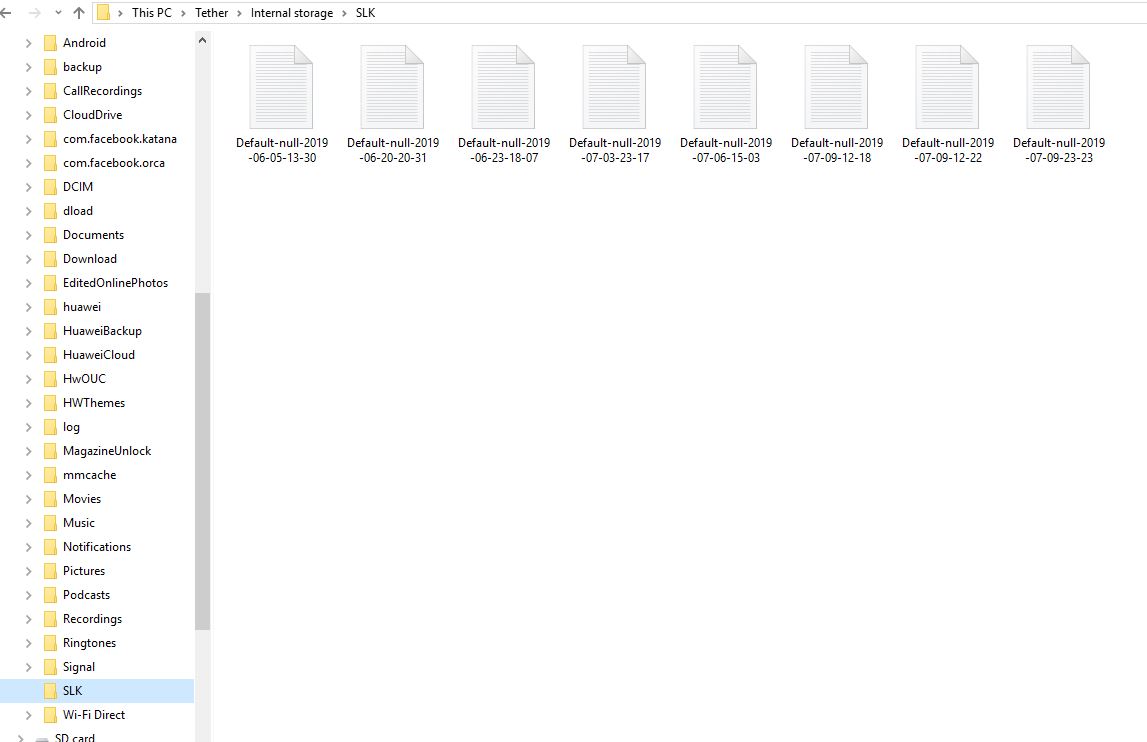
While the app functionality appears mundane, the MSmart IoT Platform is a powerful data and analytical collection platform. Examining the filesystem of the phone hosting the app, a folder named “SLK” corresponds with the with comments in the MSmart.js file, “get SLK version.” When opened in Windows File Explorer, it reveals multiple textfiles, [Figure 17]. Though difficult to read at first, it is apparent these textfiles are logs created on the phone itself when the app connects to a remote server at address https://mapp.appsmb.com, [Figure 18], Through this connection, the app sends a unique identified representing the user, and contains several fields for additional information such as a profile picture URL, the date/time of product registration, age, phone number, and sex. In the logs examined, these additional fields contained no identifying information, however research did not extend to social media platforms hosted by Instant Pot, such as their open Facebook group consisting of almost two million members [Figure 19].

Figure Overview of the Android Phone filesystem with the contents of the SLK folder expanded.



Figure Screenshot from a Windows PC of the Instant Pot Facebook Community Page

Further investigation reveals that the mapp.appsmb address resides on a MIDEA.COM.CN server under the APPSMB.COM domain, hosted by Alibaba Cloud Computing, INC [Figure 20]. According to the Instant Pot privacy policy, previously stated, all user data resides in Canada and with Amazon Web Services; however, as .cn is the country code top-level domain for the People’s Republic of China, and Alibaba Cloud Computing is an altogether separate company from Amazon Web Services, this statement is in direct conflict with actual practice.

The purpose for the data upload is unknown, however investigating the Midea IOT SDK, referenced in the app subfolder libmsmart examined previously, one encounters the GitHub page for the Midea Android IoT SDK [15]. A link at the top of the repository leads to a landing page for Midea’s IoT documentation [27], though composed entirely in a foreign language, the MSmart logo is prominently featured, and leads to the documentation for the MSmart IoT platform [Appendix B]. Using translation tools to decipher the page is necessary, however it becomes clear that one of MSmart’s main features is behavioral tracking, as mentioned in section 2.4 of their documentation.



Figure WHOIS Documentation for the MAPP.APSMB.COM URL

* 1. Contacting the Vendor

After examining the code within the control app, the content of the phone logs, and the web material for the Midea IoT SDK, an inquiry was sent to Instant Pot on July 6, 2019, directed to their Privacy Office, the contact was received and acknowledged by Instant Pot the same day, resulting in the opening of a support ticket [Figure 21].

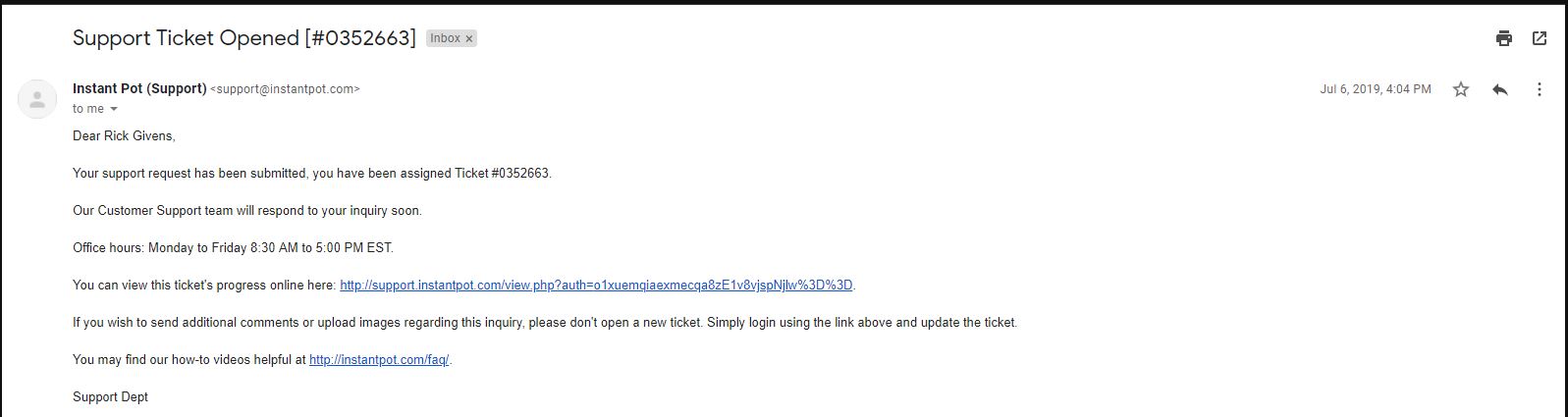


Figure Email Acknowledgement sent by Instant Pot

The inquiry requested information regarding the phone logs, and the nature of the data uploaded. Specifically, Instant Pot was asked to confirm the whether the additional form fields in the log corresponding to personal information were captured, or if they were blank for all users. Additional information was requested regarding the nature of the mapp.appsmb server, and how its physical location in the People’s Republic of China impacted the company’s assertation regarding the location of all user data .

Despite multiple follow up inquiries, no representative of Instant Pot has responded as of August 17, 2019, and the support ticket remains active.

Without clarifying information from Instant Pot, the scope, content, and nature of any data sent to Midea is unknown. However logs on the user’s phone confirm that the app connects to a Midea server in the People’s Republic of China, and uploads data via a platform that analyzes user behavior and may disclose sensitive information.

Chapter 3. Guidelines for Consumers

The information in the following subsections seeks to provide guidelines for use by consumers considering the purchase of an IoT device. Laws governing IoT devices in the United States are examined, as well as recent developments which may prompt additional scrutiny or action by governing bodies. Factors such as need and the utility of IoT devices are addressed, with a recognition that situations consumers face may vary. Finally, a set of practices which borrow heavily from enterprise information security standards are examined, and how they may relate or be applicable to the home user.

* 1. The Legal Environment

Unsurprisingly, there are few legal guidelines in the United States regarding IoT devices. While there are state laws related to data privacy and information technology, they are not consistent, nor do they have legal authority beyond the state enacting the legislature. No portion of the US Code addresses IoT security, meaning there is no consistent guideline for individual states to follow. This results in a mash of different legal definitions, preventing even simple enforcement.

The only exception is a recent amendment to California law, SB-327 Information Privacy: connected devices, effective January 1, 2020. SB-327 specifically addresses IoT security, [ ] but does not address the reasonable use and collection of data by these devices or their platforms. This is a legal gray area; questions remain regarding the control application of any IoT device and any data it collects. The control application is physically separate from the actual device, there may be difficulty in determining guidelines that address these issues. As evident in the Instant Pot WiFi Pressure Cooker, data collection is not part of the device functionality, but part of the control app residing on the user’s mobile device. In order to provide concise, consistent guidelines the control application and the IoT device must be considered as a single unit; however, if the IoT device provides its functionality without the control application, such as the Instant Pot WiFi allowing a user to enter cooking instructions manually, then this is extremely difficult as using the application may display a voluntary consent.

* 1. The Bitter Truth

Mobile device application send and receive data to users and remote servers. This data very often includes personal information and uses are variety of secure and non-secure means of transmission. Since the introduction of the first “smart” mobile devices, their distribution, use, and capabilities have grown exponentially. Within the timeframe of one human generation, a phone that can play music files has moved from the realm of novelty, to becoming a key feature for all mobile devices. The computing power has grown from the capability of a calculator to that of a full computing device allowing a user to many, if not all, the tasks performed by any modern household computer. This utility has created an environment of instant fulfillment, and instant information in which users are bombarded with content throughout their daily activities.

The novelty and convenience of instant information comes with a price. Businesses require user data so that they may deliver content to specific audiences faster than their competitors. Users require content that is tailored to their tastes delivered at speed. If a business fails to meet a user’s expectation, that user moves to a secondary provider offering similar content. The infrastructure allowing this are the users themselves.

The difficulty in governing both the IoT device and its control application as a single entity exists because the data collected by the control application is data that users freely share with other applications on their mobile device. Social media applications harvest user data, sell it to other companies, and use it to tailor both advertisement content and the user’s experience.

While the transmission of user data to a server in China appears to contradict Instant Pot’s privacy statement it is but one of several applications existing on mobile devices which transmit data. The discovery of more than one thousand Android apps operating outside of user permissions highlights this issue. Researchers from the International Computer Science Institute discovered these apps which were using various techniques to circumvent the user and access data against their wishes, [19]. The techniques involved included code within the app itself or relying upon the mutual framework of a secondary app which the user has authorized. Undoubtedly, similar circumventions or contradictions of policies and permissions by mobile application and IoT device vendors exist; it is impossible to address all of them through consumer diligence or legal governance. Users concerned with the data privacy and security of IoT devices must look beyond the device and extend that concern to other areas of their digital lives as well, otherwise, the efforts may be fruitless.

Finally, consumers must understand that data collection is not unique to devices or applications created in foreign nations but inherit in all digitally connected products in all nations. The behavior of the Instant Pot app may exist in other devices, and most likely exists in any device using a Midea wireless network adapter, but the scope of data collection by this device and its accompanying app is less than that of the social media platforms Facebook or Twitter, which are both companies based in the United States.

* 1. Determining Need Versus Novelty

With the above understanding in mind, consumers weighing a decision to purchase an IoT device must consider their actual need. For some, IoT devices offer a way of interacting with the world in a manner previously denied to them. The ability to control a thermostat or other household appliance when one is limited by their mobility or other challenges allows a degree of freedom that will greatly improve that person’s quality of life. For others the convenience of remotely accessing and controlling devices they use regularly provides valuable time savings and other advantages which render the device invaluable. Others will desire a device for its novelty, owing to its design and features. It is very easy for one to state there is no need for an IoT device, however situations differ among individuals, and the actual decision will be based entirely on the subjective perceptions of the consumer.

In weighing a purchasing decision, the consumer must decide if the necessity or positive features of an IoT device outweigh the risks associated with it. With consumer technology, the greatest risk is not a third-party gaining control of the device, but the third party already in control of the device when it is purchased. Consumers must understand that IoT devices which are granted access to information, most likely have access to related information as well. If the consumer decides to use a refrigerator with a social media application embedded as a feature, then that refrigerator will have access to the consumer’s social media account.

* 1. Understanding the Product

It is a fair statement to say most consumers will not research their potential purchases to the degree of this thesis. In fact, the evaluation of a product for purchase will most likely center on cost and the reviews of other customers. Those products with higher reviews and lower consumer costs are most likely to succeed, thus security and privacy are secondary concerns. There are however, some factors to consider.

Most important is to understand the information that the IoT device is accessing, and to thoughtfully consider the importance or necessity of that access. If the device, such as the refrigerator mentioned above, has the capability to access specific user information, then the user should both know what information is accessed, and assume that it is disclosed or uploaded to a remote computer or otherwise available to an outside party. Certain information may be trivial, however in the case of information the user considers sensitive or private, the risk of disclosure is too high. One must consider the availability of access not only to remote parties, but to other parties in the immediate area of the device. Frankly, if a consumer uses a Twitter app on their refrigerator, then the consumer must take care of sign out of the application every time it is used, else another party using the refrigerator also has access to the consumer’s Twitter account. Without knowing the specific data accessed, and how it is used, the user cannot make an informed choice without negatively impacting their digital security.

The use of default credentials is a common vulnerability among all network devices, IoT included. Default credentials are those stored with the device upon its manufacture, such as the default settings of modems and printers when they are first purchased. Common practice among device manufacturers is to host a knowledgebase website, where the default usernames and passwords of their devices are publicly available, but easy to guess nonetheless, such as admin for the username and admin for the password. Devices with hardcoded default credentials, those which the user cannot change, generally present an unacceptable risk to a user’s data privacy and security. In order to offer greater security the device must support changing the user credentials, and the user must take the initiative to change them or the device require user action to change the credentials when it is first initialized.

Another consideration is the use of encryption in the device’s transmission of data. If the device communicates with a remote computer, then the communication traffic should be encrypted. Encryption of traffic between the device and receiving computer or server helps ensure the communication is private, and decipherable only by authorized parties. This feature is harder to detect, and often the consumer must rely on the manufacturer or vendor’s own statements. In practice, though the vendor/manufacturer claims may state traffic is encrypted, this is not necessarily true. If any portion of the code transmits data in a non-secure fashion, then the entire transmission is considered non-secure regardless of other methods in place. An example of this is the Instant Pot’s control application, in which the FileTransfer.js file transmits data via an open HTTP POST method, rather than the encrypted HTTPS method. This oversight may have little impact on the security of the specific data the FileTransfer.js file is transmitting, but it calls into question other portions of the file, and whether any encryption methods used are enough to cover the shortfall. For consumers, a recommend way to determine the robustness of a device’s data encryption is to rely on technical reviews and published audits of the device and its control applications, readily available.

The use of published technical reviews, software audits and existing security research is an invaluable tool for consumers. This material provides a wealth of information regarding devices and their potential vulnerabilities, often cross-referencing multiple sources and providing conclusive results using scientifically acceptable methods. However consumers must be aware that some material is not produced directly by the publishing party and may rely upon the author’s perceptions and understanding in order to communicate the information. In all cases, the consumer should follow any reviews to their source, rather than rely on one report alone. “Following the trail” where often lead the reader through at least one additional link to the material, which may have a different perspective. By examining all available material on the subject, the consumer can develop a well-informed opinion to assist in their decisions.

* 1. Understanding the Environment

With the above considerations in mind, one must also examine the environment in which the device will operate. It is not enough to understand one device, one must understand all devices in their environment, and take the appropriate steps that are in accordance with their desired security posture. Though time consuming, the user should apply the same principals listed above to all network attached devices in their home. Worrying about one specific device and ignoring others is equivalent to applying craft glue to fix a broken windshield.

A common concern among businesses operating a network infrastructure is the introduction of unknown or unauthorized devices. To that end, effort is spent on discovering all devices attached to the organization’s network and understanding the exact nature and functionality of each device. Such steps are similarly necessary in the consumer’s home as well, though not as involved or complex as that of a business. The simplest and readily available method is to utilize the administrative dashboard of the router belonging to the consumer. Every router and Internet Service Provider (ISP) being different, the best course of action is to work with the consumer’s ISP to access the administrative dashboard, change the username and password if not done already, and then navigate to the section listing connected devices. The listed device may not make sense when first viewed, but identification becomes easier with little effort.

Chapter 4. Conclusions

The Internet of Things, while a fascinating concept of technology which will enhances the daily lives of all users and offer a degree of freedom and empowerment to millions. IoT solves problems and offers solutions ranging from simple to complex, yet it creates new challenges which are equally difficult to resolve.

This research has demonstrated a small portion of these challenges by highlighting previous incidents and threats involving IoT devices. Expanding upon that knowledge, this research delved further into the risks of IoT devices by demonstrating flaws in an arbitrarily selected device commonly available on the marketplace, and easily obtainable by any consumer.

Though there are many flaws which could affect any IoT device purchased by consumers, the greatest threat to consumer privacy and security exists in the form of targeted data collected by its accompanying control applications, which may be installed on the users’ mobile devices. These control apps may contain code which bypasses user permissions, or as in the case of the Instant Pot WiFi Pressure Cooker seek access to files on the mobile device which do not correspond to any known functionality of the application or the device itself.

While the companies which produce and distribute IoT devices do assert their compliance with consumer wishes and claim to operate out of good faith with user data, they may knowingly or unknowingly contradict themselves in practice, thus reducing their privacy policy claims to nothing more than lip service. With the various software development kits, modules, and mutual application framework present in the controlling software, it is very difficult to determine if the code contains flaws or purposely crafted functionality to access and distribute user data to third parties with which the consumer has no relationship.

When unintentional or intentional flaws or functionality affecting data security are discovered, there is limited recourse for the consumer. State laws governing the manufacture and operation of IoT devices are sparse, and within the federal jurisdiction of the United States, nonexistent. Those laws which do seek to address the functionality and data collection of IoT devices, make no mention of the controlling software application which may exist on a consumer mobile device, thus rendering the application itself to a state of legal limbo, as questions may remain regarding its inclusion as part of the definition of an IoT device, or whether it is a separate entity for purposes of enforcement. Without clear, concise definitions encompassing the device and its controlling external applications, the question creates a legal loophole which may be exploited.

Additionally, because of the lack of judicial and regulatory coverage among states and the federal government, there is little enforcement capability. Without a framework of common policies and principals across the United States, in fact, without these principles in place on a global trade level, any company outside the jurisdiction of a governing organization has no expectation of consequence and only has its own internal policies governing its actions. These policies, when contradicted or violated, offer little to no recourse for consumer relief.

The issues of regulation and enforcement aside, consumers should not expect total data privacy. The use of mobile technology has become a daily facet of civilization, and the willingness of its users to engage in online activity prevents any expectation of total privacy without a drastic change in behavior.

The best solution for consumers contemplating an IoT purchase is to weigh their need or perceived need versus the risks posed by the device. Devices purchase for the sheer novelty of owning them may offer limited utility beyond that offered by a standard non-IoT version. Consumers must understand that any device granted access to their data will send that data to a third party.

Consumers must understand the product, and how it operates. This understanding of the product extends to the functionality any controlling application and moves beyond the considerations of price and market reviews. Consumers must know if the device is subject common vulnerabilities, such as hard coded network credentials which cannot be changed, or those that are not hard coded, but have not been changed. They must understand how the data transmitted by the device or its application is handled, either encrypted or unencrypted, and they must educate themselves by researching the device prior to purchase for any previously reported issues, risks, or vulnerabilities. This level of diligence is not far beyond the normal considerations of a consumer when making an informed purchasing decision, rather it extends the considerations only slightly. By reading technical reviews following a scientific method, and following stories to their cited sources to eliminate author bias, a consumer can examine facts surrounding a device, or for that matter any product or subject of which they have interest.

The final consideration for consumers is the environment in which the device operates. Mentioned previously, consumers must understand that diligence on one device will not prevent other devices and services from disclosing data or introducing a vulnerability. A security minded consumer with default credentials on a home router, or multiple IoT devices previously purchased without evaluation will have no expectation of security or privacy.

Ultimately, there is no guarantee of total data privacy or total freedom of vulnerability or other risk. As technology evolves, new vulnerabilities are introduced, or methods discovered which bypass safeguards. The accumulation of devices and services, all accessing data, prevents a total or perfect solution. Consumers must understand that the number of devices and services increases the risk of exposure proportionately; in order to reduce the risk the recommended guidelines must apply to all devices and accompany a change in behavior.

Bibliography

[1] Ali, Bako, and Ali Ismail Awad. “Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes.” US National Laboratory of Medicine and National Institutes of Health, MDPI, 8 Mar. 2018, www.ncbi.nlm.nih.gov/pubmed/29518023. Accessed May 19, 2019.

[3] Franceschi-Bicchierai, Lorenzo. “How Hackers Could Steal Your Cellphone Pictures From Your IoT Crock-Pot.” Vice, VICE, 2 Nov. 2016, www.vice.com/en\_us/article/wnx7n9/how-hackers-could-steal-your-cellphone-pictures-from-your-iot-crock-pot. Accessed 4 Jun. 2019.

[4] Fruhlinger, Josh. “The Mirai Botnet Explained: How IoT Devices Almost Brought down the Internet.” CSO Online, CSO, 9 Mar. 2018, www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html. Accessed 4 Jun. 2019.

[5] History of Computers, The University of Rhode Island Department of Computer Science and Statistics, homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading03.htm. Accessed May 19, 2019.

[6] “Instant Pot Smart WiFi 6 Quart Multi-Use Electric Pressure, Slow, Rice Cooker, Yogurt, Cake Maker, Sauté, Steamer and Warmer, Silver.” Amazon, Amazon, www.amazon.com/Instant-Pot-Smart-Electric-Pressure/dp/B0777XQ4S8?ref\_=bl\_dp\_s\_web\_3031632011. Accessed May 19, 2019.

[7] “Instant Pot Smart Wifi.” Instant Pot, instantpot.com/portfolio-item/instant-pot-smart-wifi/. Accessed May 19, 2019.

[8] “IoT: Number of Connected Devices Worldwide 2012-2025.” Statista, www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed 4 Jun. 2019.

[9] Jr., Tom Huddleston. “These Chinese Hackers Tricked Tesla's Autopilot into Suddenly Switching Lanes.” CNBC, CNBC, 3 Apr. 2019, www.cnbc.com/2019/04/03/chinese-hackers-tricked-teslas-autopilot-into-switching-lanes.html. Accessed 4 Jun. 2019.

[10] Korolov, Maria. “What Is a Botnet? And Why They Aren't Going Away Anytime Soon.” CSO Online, CSO, 27 Feb. 2019, www.csoonline.com/article/3240364/what-is-a-botnet-and-why-they-arent-going-away-anytime-soon.html. Accessed 4 Jun. 2019.

[11] Kumar, Kalyan. “Tesla Model S Update Causes Performance Bug, Struggles With Limited Power.” International Business Times, 9 May 2019, www.ibtimes.com/tesla-model-s-update-causes-performance-bug-struggles-limited-power-2790824. Accessed 4 Jun. 2019.

[12] “LG Electronics Introduces Digital Refrigerator.” Appliance Design Magazine RSS, www.appliancedesign.com/articles/89516-lg-electronics-introduces-digital-refrigerator. Accessed 13 May 2017.

[13] Mariani, Joe. “Guiding the IoT to Safety.” Deloitte Insights, www2.deloitte.com/insights/us/en/focus/internet-of-things/regulating-iot-technology-role-of-government.html. Accessed May 19, 2019.

[14] Maheshwari, Sapna. “Burger King 'O.K. Google' Ad Doesn't Seem O.K. With Google.” The New York Times, The New York Times, 12 Apr. 2017, www.nytimes.com/2017/04/12/business/burger-king-tv-ad-google-home.html. Accessed 4 Jun. 2019.

[15] Midea-Sdk-Org. “Midea-Sdk-Org/Android-Sdk.” GitHub, 13 Sept. 2017, github.com/midea-sdk-org/android-sdk. Accessed 1 July 2019.

[16] FCC ID “Midea Smart Technology Co., LTD, Wi-Fi Module 0004,” Searchable FCC ID Database. <https://fccid.io/2AIRV0004>. Accessed 16 Jul. 2019

[17] “M\*Smart.” http://iot.midea.com

[18] NCCIC. “Security Tip (ST04-015).” US CERT Security Tip (ST-015)O, United States Department of Homeland Security, 4 Nov. 2009, www.us-cert.gov/ncas/tips/ST04-015. Last Revision June 28, 2018. Accessed 4 Jun. 2019.

[19] Ng, Alfred. “More than 1,000 Android Apps Harvest Data Even after You Deny Permissions.” CNET, CNET, 8 July 2019, [www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/](http://www.cnet.com/news/more-than-1000-android-apps-harvest-your-data-even-after-you-deny-permissions/). Accessed 12 July 2019.

[20] “Over 50 Years of Moore's Law.” Intel, www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html. Accessed 10 Jun. 2019.

[21] “Overview.” Architectural Overview of Cordova Platform - Apache Cordova, cordova.apache.org/docs/en/latest/guide/overview/index.html. Accessed 19 July 2019.

[22] Price, Rob. “Nearly Half a Million Peoples' Pacemakers Are at Risk of Being Hacked.” Business Insider, Business Insider, 31 Aug. 2017, www.businessinsider.com/465000-pacemakers-hacking-us-fda-recall-firmware-update-2017-8.

[23] “Privacy Policy.” Instant Pot, Instant Brands, Inc., instantpot.com/privacy-policy-instant-pot/. Accessed 17 July. 2019.

[24] Raposo, Kevin. “Hackers Have Found a Way to Hack Your IoT Crock-Pot.” KnowTechie, 2 Nov. 2016, knowtechie.com/connected-crock-pot-hotbed-hackers/. Accessed 4 Jun. 2019.

[25] Ruß-Mohl, Stephan. Die Informierte Gesellschaft Und Ihre Feinde Warum Die Digitalisierung Unsere Demokratie gefährdet. Herbert Von Halem Verlag, 2017. Accessed May 19, 2019.

[26] “Smart WiFi 60 Pairing.” Instant Pot, instantpot.com/smart-wifi-60-pairing/#tab-id-2. Accessed May 19, 2019.

[27] “Smart开放平台.” MSmart, iot.midea.com/. Accessed 1 July 2019.

[28] Vaas, Lisa. “Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking.” Naked Security, 22 Oct. 2013, nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/. Accessed 4 Jun. 2019.

[29] Vaughan-Nichols, Steven J. “Tesla Starts to Release Its Cars' Open-Source Linux Software Code.” ZDNet, ZDNet, 18 Jan. 2019, www.zdnet.com/article/tesla-starts-to-release-its-cars-open-source-linux-software-code/. Accessed 4 Jun. 2019.

[30] Welcome to Midea Global, www.midea.com/global/technology\_innovation/technology\_introduction/. Accessed 16 Jul. 2019.

[31] “What Is a Man-in-the-Middle Attack?” Official Site, us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html. Accessed 4 Jun. 2019.

[32] “What Is an Access Point and How Is It Different from a Range Extender?” Linksys, www.linksys.com/us/r/resource-center/what-is-a-wifi-access-point/. Accessed 4 Jun. 2019.

[33] “Wi-Fi Alert: The Evil Twins of Access Points.” Panda Security Mediacenter, 8 Jan. 2019, www.pandasecurity.com/mediacenter/security/wifi-evil-twins-access-points/. Accessed 4 Jun. 2019.

Appendix A: Unformatted Log Sample from the SLK Folder

I 2019-07-06 15:03:57.104 (SLK: :[fd$a.run(Line:209)]) Server connection ok.....

I 2019-07-06 15:03:57.105 (SLK: :[fd$a.run(Line:209)]) Server connection ok......

D 2019-07-06 15:03:57.105 (SLK: :[MSmartUserManagerProxy.loginWithAccount(Line:119)]) loginWithAccount: user-622960.45e109dddc@msmart.instantpot.com

I 2019-07-06 15:03:57.105 (SLK: :[v.a(Line:210)]) /v1/user/login/id/getappId=1201&clientType=1&format=2&language=en\_US&loginAccount=user-622960.45e109dddc@msmart.instantpot.com&src=201&stamp=20190706150356d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:03:57.105 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:03:57.105 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/user/login/id/get? {loginAccount=user-622960.45e109dddc%40msmart.instantpot.com&clientType=1&src=201&appId=1201&format=2&sign=8f8b04aec71ba534003cf7fcec15669b112191f3650955d1fb513582714f8917&stamp=20190706150356&language=en\_US}

I 2019-07-06 15:03:57.105 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/user/login/id/get

I 2019-07-06 15:03:57.105 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","result":{"loginId":"9d39a936-65b2-4987-84b3-37d5764c7d31"},"errorCode":"0"}]

I 2019-07-06 15:03:57.105 (SLK: :[v.a(Line:210)]) /v1/user/loginappId=1201&clientType=1&format=2&iampwd=ff0befc6a428a4db1e8657bee873672fe5a4674379a19530d95df7097cb3a167&language=en\_US&loginAccount=user-622960.45e109dddc@msmart.instantpot.com&password=e6093bd426c130deba942699d040fb782f5739115ecabd957c445a093e861938&pushToken=d7LkBuHFydM:APA91bE\_LxhVjH4XvB0SCNlxapvshPtyxdIYKt6qO\_tWFGLLBQNMLFIgkkOrR8pwJUxpZEuNqsNtjy5w85N3Tu77BwCBOjHN7hvAQmlEn9nL1FoNMKCXoQ03pBC6DIAFaZ2sjPDlYXeS&pushType=4&src=201&stamp=20190706150356d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:03:57.105 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:03:57.105 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/user/login? {loginAccount=user-622960.45e109dddc%40msmart.instantpot.com&src=201&format=2&sign=5a58b34bb339cc98d3ea1fbae4fd7f1a3d7157352486bd17638e7ef2061b2deb&stamp=20190706150356&language=en\_US&pushToken=d7LkBuHFydM%3AAPA91bE\_LxhVjH4XvB0SCNlxapvshPtyxdIYKt6qO\_tWFGLLBQNMLFIgkkOrR8pwJUxpZEuNqsNtjy5w85N3Tu77BwCBOjHN7hvAQmlEn9nL1FoNMKCXoQ03pBC6DIAFaZ2sjPDlYXeS&pushType=4&password=e6093bd426c130deba942699d040fb782f5739115ecabd957c445a093e861938&clientType=1&appId=1201&iampwd=ff0befc6a428a4db1e8657bee873672fe5a4674379a19530d95df7097cb3a167}

I 2019-07-06 15:03:57.105 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/user/login

I 2019-07-06 15:03:57.105 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","result":{"originPrivateVersion":"","nickname":"user-622960.45e109dddc@msmart.instantpot.com","sessionId":"9f7619a3b6ad4d499c118ab90165fd9020190706200356894","accessToken":"42facc7bfff7af3c10bf25698977aac0dc9a518a45b7d606d4c07ce5208566a2","userId":"1593940","versionCode":"","leftCount":""},"errorCode":"0"}]

D 2019-07-06 15:03:57.105 (SLK: :[bM.a(Line:1184)]) Handle login success internal event!

I 2019-07-06 15:03:57.105 (SLK: :[ap.handleMessage(Line:308)]) Handle login success internal event!

I 2019-07-06 15:03:57.105 (SLK: :[bM.a(Line:1215)]) Sync davicafter login success!

I 2019-07-06 15:03:57.105 (SLK: :[an.g(Line:211)]) Sync davicafter login success!

D 2019-07-06 15:03:57.106 (SLK: ProtocolControlManager:[bg.a(Line:161)]) Init protocol control manager

I 2019-07-06 15:03:57.106 (SLK: :[bM.a(Line:1236)]) Begin request data

I 2019-07-06 15:03:57.106 (SLK: :[v.a(Line:210)]) /v1/appliance/type/list/getapplianceType=0xFF&format=2&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894&src=201&stamp=20190706150357d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:03:58.141 (SLK: :[v.a(Line:210)]) /v1/user/info/getformat=2&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894&src=201&stamp=20190706150357d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:03:58.141 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:03:58.141 (SLK: :[v.a(Line:210)]) /v1/appliance/user/list/getformat=2&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894&src=201&stamp=20190706150357d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:03:58.141 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:03:58.141 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:03:58.141 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/user/info/get? {src=201&format=2&sign=1c964affb697caf4f0e19a215d34465901054233d637361efdd399e1aede2b69&stamp=20190706150357&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894}

I 2019-07-06 15:03:58.141 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/appliance/type/list/get? {src=201&format=2&applianceType=0xFF&sign=43f098de28b01b5876e29f573b407d9298ac2965b20d5cc552907fcd9d7c7576&stamp=20190706150357&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894}

I 2019-07-06 15:03:58.141 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/appliance/user/list/get? {src=201&format=2&sign=ae4a0018a44f3bd0c9998a4e855cfc481e3d82b577299b5c337d969b425d06f8&stamp=20190706150357&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894}

I 2019-07-06 15:03:58.142 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/user/info/get

I 2019-07-06 15:03:58.142 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","result":{"uid":"","address":"","profilePicUrl":"","phone":"","registerTime":"2019-06-03 01:05:04","signature":"","sex":"","nickname":"user-622960.45e109dddc@msmart.instantpot.com","mobile":"","id":"1593940","email":"user-622960.45e109dddc@msmart.instantpot.com","age":""},"errorCode":"0"}]

I 2019-07-06 15:03:58.142 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/appliance/user/list/get

I 2019-07-06 15:03:58.142 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","result":{"list":[{"onlineStatus":"0","type":"0xEC","homegroupId":"","userId":"1593940","des":"","activeStatus":"1","homegroupCreateUserId":"","wifiVersion":"","name":"Instant\_Pot","modelNumber":"22","homegroupNumber":"","id":"14293651199656","sn":"4a1ddcb30471b3cceafbfd0348d09d18b0fe8eeb243e7bda4d1dcf35684164acf30bc7af2086a44e0df050a1da544e44","userType":"1"}]},"errorCode":"0"}]

I 2019-07-06 15:03:58.142 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/appliance/type/list/get

I 2019-07-06 15:03:58.142 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","result":{"list":[{"des":"smart socket","name":"smart socket","id":"1","type":"0x10"},{"des":"Smart Remote","name":"Smart Remote","id":"2","type":"0x11"},{"des":"Sensor Box","name":"Sensor Box","id":"3","type":"0x12"},{"des":"Smart Lighting","name":"Smart Lighting","id":"4","type":"0x13"},{"des":"Smart Curtain","name":"Smart Curtain","id":"5","type":"0x14"},{"des":"Smart Router","name":"Smart Router","id":"6","type":"0x1B"},{"des":"Air Conditioner","name":"Air Conditioner","id":"7","type":"0xAB"},{"des":"AC","name":"AC","id":"8","type":"0xAC"},{"des":"Microwave Oven","name":"Microwave Oven","id":"9","type":"0xB0"},{"des":"Oven","name":"Oven","id":"10","type":"0xB1"},{"des":"Steamer Oven","name":"Steamer Oven","id":"11","type":"0xB2"},{"des":"Disinfection Cabinet","name":"Disinfection Cabinet","id":"12","type":"0xB3"},{"des":"Small Toaster","name":"Small Toaster","id":"13","type":"0xB4"},{"des":"Intelligent Cupboard","name":"Intelligent Cupboard","id":"14","type":"0xBA"},{"des":"Hood","name":"Hood","id":"15","type":"0xB6"},{"des":"Hob","name":"Hob","id":"16","type":"0xB7"},{"des":"Vacuum Cleaner","name":"Vacuum Cleaner","id":"17","type":"0xB8"},{"des":"Induction","name":"Induction","id":"18","type":"0xB9"},{"des":"Refrigerator","name":"Refrigerator","id":"20","type":"0xCA"},{"des":"CAC","name":"CAC","id":"21","type":"0xCC"},{"des":"Heating water pump heater system","name":"Heating water pump heater system","id":"22","type":"0xCD"},{"des":"loading washing machine","name":"Top","id":"23","type":"0xDA"},{"des":"loading washing machine","name":"Front","id":"24","type":"0xDB"},{"des":"dryer","name":"dryer","id":"25","type":"0xDC"},{"des":"Dishwasher","name":"Dishwasher","id":"26","type":"0xE1"},{"des":"Electrical water heater","name":"Electrical water heater","id":"27","type":"0xE2"},{"des":"Gas water heater","name":"Gas water heater","id":"28","type":"0xE3"},{"des":"Aqua Energy system","name":"Aqua Energy system","id":"29","type":"0xE4"},{"des":"Rice Cooker","name":"Rice Cooker","id":"30","type":"0xEA"},{"des":"Electromagnetic Oven","name":"Electromagnetic Oven","id":"31","type":"0xEB"},{"des":"Electric Pressure Cooker","name":"Electric Pressure Cooker","id":"32","type":"0xEC"},{"des":"Purifying Machine","name":"Purifying Machine","id":"33","type":"0xED"},{"des":"Soymilk Maker","name":"Soymilk Maker","id":"34","type":"0xEF"},{"des":"Cooling Fan","name":"Cooling Fan","id":"35","type":"0x90"},{"des":"fan","name":"fan","id":"36","type":"0xFA"},{"des":"Heater","name":"Heater","id":"37","type":"0xFB"},{"des":"Heater","name":"Heater","id":"38","type":"0xFC"},{"des":"Humidifier","name":"Humidifier","id":"39","type":"0xFD"},{"des":"Air Conditioner Fan","name":"Air Conditioner Fan","id":"40","type":"0xFE"},{"des":"Broadcasting Appliances type (All appliances can receive)","name":"Broadcasting Appliances type (All appliances can receive)","id":"41","type":"0xFF"},{"des":"Dehumidifier","name":"Dehumidifier","id":"42","type":"0xA1"},{"des":"Microwave steam oven","name":"Microwave steam oven","id":"44","type":"0xB5"},{"des":"","name":"AirHousekeeper","id":"45","type":"0x01"},{"des":"","name":"NutritionHousekeeper","id":"46","type":"0x02"},{"des":"","name":"WaterHousekeeper","id":"47","type":"0x03"},{"des":"","name":"Security","id":"48","type":"0x04"},{"des":"","name":"energy","id":"49","type":"0x05"},{"des":"","name":"entertainment","id":"50","type":"0x06"},{"des":"","name":"null","id":"51","type":"0xC7"},{"des":"","name":"null","id":"52","type":"0xC8"},{"des":"","name":"null","id":"53","type":"0xC9"},{"des":"","name":"null","id":"54","type":"0xE9"},{"des":"Slow Cooker","name":"Slow Cooker","id":"55","type":"0xE8"},{"des":"","name":"jiqiren","id":"56","type":"0x28"},{"des":"","name":"MSmart","id":"60","type":"0x00"},{"des":"","name":"","id":"61","type":"0xDD"},{"des":"","name":"","id":"62","type":"0xF1"},{"des":"","name":"","id":"63","type":"0xF0"},{"des":"","name":"","id":"64","type":"0x

I 2019-07-06 15:03:58.142 (SLK: :[fg$a.a(Line:410)]) 15"},{"des":"","name":"unknown","id":"65","type":"0xBB"},{"des":"","name":"Coffeemaker","id":"66","type":"0xF2"},{"des":"","name":"sensors","id":"67","type":"0xBC"},{"des":"","name":"Smart gateway","id":"68","type":"0x16"},{"des":"","name":"Air box","id":"69","type":"0xAD"},{"des":"","name":"Electromagnetic","id":"70","type":"0xE7"},{"des":"","name":"","id":"79","type":"0xD0"},{"des":"","name":"","id":"80","type":"0x50"},{"des":"","name":"Hanging furnace","id":"81","type":"0xE6"},{"des":"Kitchen Scale","name":"Kitchen Scale","id":"82","type":"0xC0"},{"des":"","name":"Garbage Grinder","id":"83","type":"0x22"},{"des":"Central heating water heater","name":"Central heating water heater","id":"84","type":"0xC3"}]},"errorCode":"0"}]

I 2019-07-06 15:03:58.142 (SLK: :[bM.a(Line:1246)]) Sync device type data success!

I 2019-07-06 15:03:58.142 (SLK: :[bM.a(Line:1267)]) Sync user info success!

I 2019-07-06 15:03:58.142 (SLK: :[bM.a(Line:1297)]) Sync user device list success!

D 2019-07-06 15:03:58.142 (SLK: sstwzs:[bw.c(Line:255)]) Sync data after login coast time: 1087getDeviceBySn sn:0000EC1110002001618B081110430000

I 2019-07-06 15:03:58.142 (SLK: :[bM.a(Line:1348)]) Sync data after login coast time: 1087getDeviceBySn sn:0000EC1110002001618B081110430000

D 2019-07-06 15:03:58.687 (SLK: :[aD.run(Line:1165)]) 设置device sn = 0000EC1110002001618B081110430000 deviceId:1429365119965

I 2019-07-06 15:03:58.687 (SLK: :[cr.a(Line:179)]) SLK initialization success

D 2019-07-06 15:03:58.687 (SLK: :[aD.run(Line:1167)]) device == null sn =0000EC1110002001618B081110430000

D 2019-07-06 15:03:58.687 (SLK: sstwzs:[bw.a(Line:4198)]) getTokenAndK1FromCloud device:com.midea.iot.sdk.bv@eecf6e5 sn:0000EC1110002001618B081110430000 udpkey:06520be0914eab2acdb414ac87cfe748

I 2019-07-06 15:03:58.687 (SLK: :[v.a(Line:210)]) /v1/iot/secure/getTokenformat=2&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894&src=201&stamp=20190706150358&udpid=06520be0914eab2acdb414ac87cfe748d02baa9d8e05a213bea9f20069a7b149

D 2019-07-06 15:03:58.687 (SLK: :[MSmartUserManagerProxy.searchUserByAccount(Line:277)]) searchUserByAccount: user-622960.45e109dddc@msmart.instantpot.com

I 2019-07-06 15:03:58.687 (SLK: :[v.a(Line:210)]) /v1/user/account/searchformat=2&language=en\_US&loginAccount=user-622960.45e109dddc@msmart.instantpot.com&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894&src=201&stamp=20190706150358d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/user/account/search? {loginAccount=user-622960.45e109dddc%40msmart.instantpot.com&src=201&format=2&sign=1db201e0773ea782345c044d9eba49b9dd99284185f3c456d36d2726c0bfa5b7&stamp=20190706150358&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894}

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/iot/secure/getToken? {udpid=06520be0914eab2acdb414ac87cfe748&src=201&format=2&sign=a89953f552a51dae5bd29e3b8f73d1783869fb2f1fc674310bf206ce6c2b6810&stamp=20190706150358&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894}

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/iot/secure/getToken

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/iot/secure/getToken

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"result":{"tokenlist":[{"udpId":"06520be0914eab2acdb414ac87cfe748","key":"38A0B550008947E5B94C053AA5F37307815C3AF34A3640CF8A525ACAC9B4891C","token":"945B9EA774F5C970CAB03B3A3AF5AC6A00D156A59EB3326CA1CA1F4D08ED9A8F7BE21EA1987D3BC7EE6D9E1EA1E759F6F972555B48814A8CEFF13667B84337E4"}]},"msg":"ok","errorCode":"0"}]

E 2019-07-06 15:03:58.688 (SLK: :[bx.a(Line:208)]) sendToCloudBySDK isSuccess

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","result":{"address":"","profilePicUrl":"","phone":"","signature":"","registerTime":"2019-06-03 01:05:04","sex":"","nickname":"user-622960.45e109dddc@msmart.instantpot.com","mobile":"","id":"1593940","email":"user-622960.45e109dddc@msmart.instantpot.com","age":""},"errorCode":"0"}]

I 2019-07-06 15:03:58.688 (SLK: :[cl.a(Line:495)]) Request search user success!

D 2019-07-06 15:03:58.688 (SLK: :[MSmartUserManagerProxy.searchUserByAccount(Line:277)]) searchUserByAccount: user-622960.45e109dddc@msmart.instantpot.com

I 2019-07-06 15:03:58.688 (SLK: :[v.a(Line:210)]) /v1/user/account/searchformat=2&language=en\_US&loginAccount=user-622960.45e109dddc@msmart.instantpot.com&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894&src=201&stamp=20190706150358d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:03:58.688 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:04:24.481 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/user/account/search? {loginAccount=user-622960.45e109dddc%40msmart.instantpot.com&src=201&format=2&sign=1db201e0773ea782345c044d9eba49b9dd99284185f3c456d36d2726c0bfa5b7&stamp=20190706150358&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894}

I 2019-07-06 15:04:24.481 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/user/account/search

I 2019-07-06 15:04:24.481 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","result":{"address":"","profilePicUrl":"","phone":"","signature":"","registerTime":"2019-06-03 01:05:04","sex":"","nickname":"user-622960.45e109dddc@msmart.instantpot.com","mobile":"","id":"1593940","email":"user-622960.45e109dddc@msmart.instantpot.com","age":""},"errorCode":"0"}]

I 2019-07-06 15:04:24.481 (SLK: :[cl.a(Line:495)]) Request search user success!

D 2019-07-06 15:04:24.481 (SLK: :[MSmartUserDeviceManagerProxy.syncCloudData(Line:809)]) syncCloudData

I 2019-07-06 15:04:24.481 (SLK: :[bM.b(Line:1472)]) Sync data after login success!

I 2019-07-06 15:04:24.481 (SLK: :[bM.b(Line:1475)]) Begin request data

I 2019-07-06 15:04:24.481 (SLK: :[v.a(Line:210)]) /v1/appliance/user/list/getformat=2&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894&src=201&stamp=20190706150359d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:04:24.481 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:04:24.481 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/appliance/user/list/get? {src=201&format=2&sign=180d0b037846c4ea7ecd4d913f33701c038321c2fddd3baad516400ce6fee58f&stamp=20190706150359&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894}

I 2019-07-06 15:04:24.481 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/appliance/user/list/get

I 2019-07-06 15:04:24.481 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","result":{"list":[{"onlineStatus":"0","type":"0xEC","homegroupId":"","userId":"1593940","des":"","activeStatus":"1","homegroupCreateUserId":"","wifiVersion":"","name":"Instant\_Pot","modelNumber":"22","homegroupNumber":"","id":"14293651199656","sn":"4a1ddcb30471b3cceafbfd0348d09d18b0fe8eeb243e7bda4d1dcf35684164acf30bc7af2086a44e0df050a1da544e44","userType":"1"}]},"errorCode":"0"}]

I 2019-07-06 15:04:24.482 (SLK: :[bM.b(Line:1480)]) Sync user device list success!

D 2019-07-06 15:04:24.482 (SLK: sstwzs:[bw.c(Line:255)]) getDeviceBySn sn:0000EC1110002001618B081110430000Sync data after login coast time: 494

I 2019-07-06 15:04:24.482 (SLK: :[bM.b(Line:1525)]) getDeviceBySn sn:0000EC1110002001618B081110430000Sync data after login coast time: 494

D 2019-07-06 15:04:24.482 (SLK: :[aD.run(Line:1165)]) 设置device sn = 0000EC1110002001618B081110430000 deviceId:1429365119965

D 2019-07-06 15:04:24.482 (SLK: :[MSmartUserDeviceManagerProxy.getAllDeviceList(Line:52)]) getAllDeviceList

I 2019-07-06 15:04:24.482 (SLK: :[ap.handleMessage(Line:308)]) Send scan device broadcast..........20000

I 2019-07-06 15:04:24.482 (SLK: :[an.g(Line:211)]) Send device scan broadcast...

I 2019-07-06 15:04:24.482 (SLK: :[ap.handleMessage(Line:308)]) Send scan device broadcast..........20000

I 2019-07-06 15:06:33.036 (SLK: :[an.g(Line:211)]) Send device scan broadcast...

D 2019-07-06 15:06:33.037 (SLK: :[MSmartUserManagerProxy.updateUserSession(Line:322)]) updateUserSession

I 2019-07-06 15:06:33.037 (SLK: :[v.a(Line:210)]) /v1/user/session/updateformat=2&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894&src=201&stamp=20190706150424d02baa9d8e05a213bea9f20069a7b149

I 2019-07-06 15:06:33.037 (SLK: :[fg$a.b(Line:296)]) Connect midea cloud server!

I 2019-07-06 15:06:33.037 (SLK: :[fg$a.b(Line:4524)]) https://mapp.appsmb.com/v1/user/session/update? {src=201&format=2&sign=aac42e11ea0737bc5ef174977947004cb9579790d10645d841a4b9b109b7d2e3&stamp=20190706150424&language=en\_US&sessionId=9f7619a3b6ad4d499c118ab90165fd9020190706200356894}

I 2019-07-06 15:06:33.037 (SLK: :[fg$a.a(Line:409)]) Request:https://mapp.appsmb.com/v1/user/session/update

I 2019-07-06 15:06:33.037 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response: {"msg":"ok","errorCode":"0"}]

I 2019-07-06 15:06:33.037 (SLK: :[cm.a(Line:561)]) Update user session success!

I 2019-07-06 15:06:33.037 (SLK: :[ap.handleMessage(Line:308)]) Send scan device broadcast..........20000

I 2019-07-06 15:06:33.037 (SLK: :[an.g(Line:211)]) Send device scan broadcast...

I 2019-07-06 15:06:33.038 (SLK: :[ap.handleMessage(Line:308)]) Send scan device broadcast..........20000

I 2019-07-06 15:06:33.038 (SLK: :[an.g(Line:211)]) Send device scan broadcast...

I 2019-07-06 15:06:33.038 (SLK: :[ap.handleMessage(Line:308)]) Send scan device broadcast..........20000

I 2019-07-06 15:06:33.038 (SLK: :[an.g(Line:211)]) Send device scan broadcast...

I 2019-07-06 15:06:33.038 (SLK: :[ap.handleMessage(Line:308)]) Send scan device broadcast..........20000

I 2019-07-06 15:06:33.038 (SLK: :[an.g(Line:211)]) Send device scan broadcast...

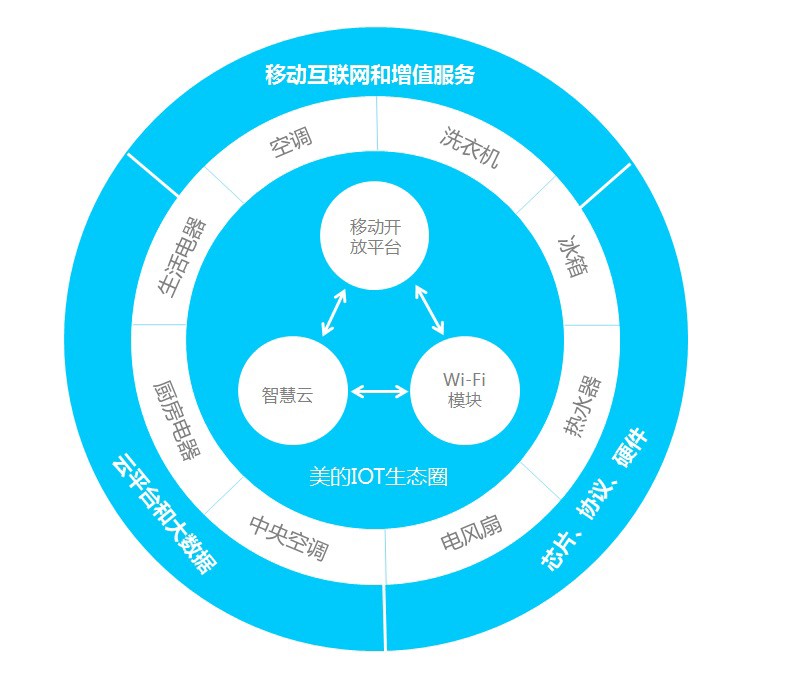
I 2019-07-06 15:06:33.038 (SLK: :[ap.handleMessage(Line:308)]) Send scan device broadcast..........20000

I 2019-07-06 15:06:33.038 (SLK: :[an.g(Line:211)]) Send device scan broadcast...

I 2019-07-06 15:06:33.038 (SLK: :[ap.handleMessage(Line:308)]) Send scan device broadcast..........20000

I 2019-07-06 15:06:33.038 (SLK: :[an.g(Line:211)]) Send device scan broadcast...

Appendix B: Translation of the Midea IoT SDK Msmart Documentation



**Overview**

M-Smart is a "one-stop, fully managed" intelligent IoT platform based on the smart cloud of the United States, integrating all kinds of home appliances, smart items and smart sets of products, providing access, object analysis, object management, big data. A series of IoT core products and services help developers quickly realize the interaction between users and devices, devices and devices, devices and users.

It is hoped that through continuous technological innovation and continuous accumulation of industry experience, Smart Cloud Platform will increasingly become a smart Internet of Things platform that understands the industry and provides complete solutions for home appliances, home, automotive, real estate and other industries. At the same time, based on the M-Smart certification service, an eco- cooperation mechanism of mutual trust and win-win is established to help industry users quickly realize the commercial value of the Internet of Everything.

**Ecosphere**

## Platform advantage



1. **IoT chip / module access**
   1. **IoT chip / module introduction**

### Introduction to M-Smart Embedded Solution

Midea Smart Cloud provides an embedded M-Smart solution for IoT chips/modules, including convenient and efficient wireless configuration management, end-to-cloud secure channel connection management, terminal login activation and deregistration management, M-Smart protocol management, and Tripartite agreement conversion, etc. The IoT chips/modules that currently support the M-Smart solution include Wi-Fi, 2G, 3G, bluetooth, zigbee and other communication types.

### M-Smart Embedded Solution Integration

IoT chip/module vendors can learn about the M-Smart solution system and access related processes at this site. After confirming the cooperation intention and signing the agreement, you can download the SDK package and related technical documents from the site development center. If you have any questions, you can contact us by contacting us.

### M-Smart chip/module certification

集成M-Smart物联解决方案的芯片/模组需要通过相关的认证测试。认证流程由芯片/模组商自主发起，美的智慧 家居或者第三方测试机构负责测试验收。通过M-Smart认证测试的芯片及模组方可获得美的颁发的M-Smart认证 书，并且可以在M-Smart官网的成功案例处显示。

### 1.1.4 M-Smart芯片/模组产品线



**1.2 IoT芯片/模组接入模式**

**1.2.1Wi-Fi模组方案集成**

美的智能为Wi-Fi模组提供M-Smart SDK包，集成的功能包含：智能云连接管理及物联业务服务、Wi-Fi配网模块

（支持一键配置及热点方案）、OTA升级管理、设备本地配置管理等。另外目前与智能套装集合，可以与家庭其它 智能设备进行联动控制与信息推送。

Wi-Fi模组集成M-Smart方案示意图如下：



### 1.2.2 WiFi模组接入模式

目前WIFI模块合作方式有两大类，第一类属于家电互动，家电类互动有以下几种合作方式： 合作方式A:

美的智慧家居提供成熟的M-Smart通讯模块，提供公版的APP用于生产调试和DEMO演示； 产品接入美的云平台，同时支持接入其他云平台，例如阿里、京东等。

合作方式B:

美的智慧家居提供成熟的M-Smart通讯模块，提供公版的APP用于生产调试和DEMO演示； 不接入美的云，只支持接入第三方云平台，例如自建云、阿里、京东等。

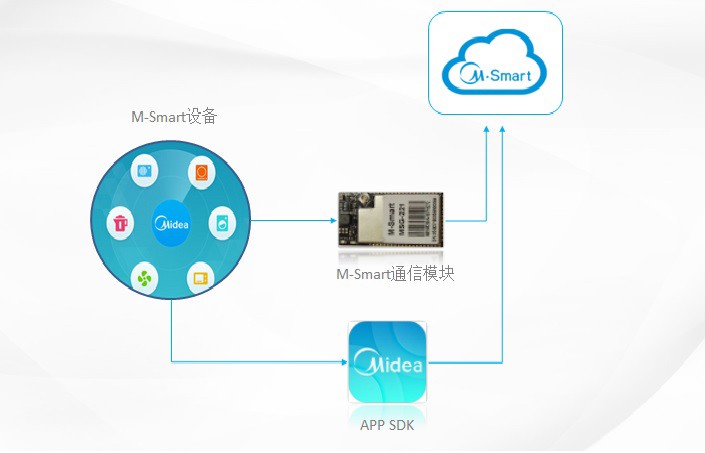
合作方式C:

美的智慧家居提供通讯模块硬件，不含软件； 这种合作模式适用于有开发能力的企业，例如方案公司。

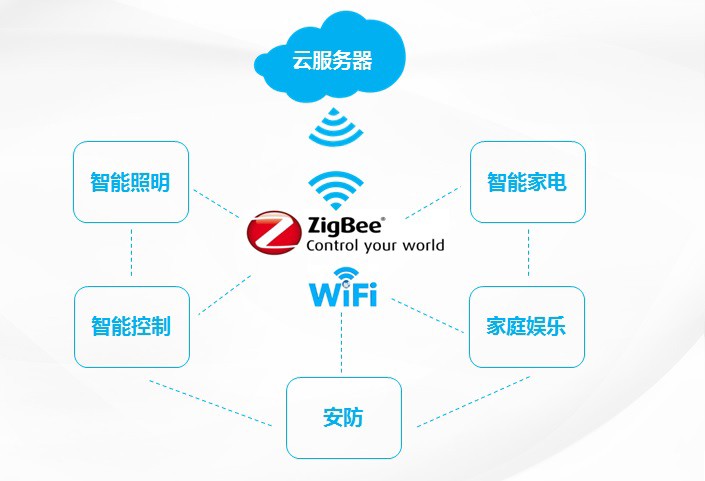
合作方式D:

美的智慧云方案整体部署到第三方企业； 通讯模块直接向美的智慧家居采购；

智慧家居提供SDK给第三方企业，开发自己的移动APP（或者由智慧家居定制开发APP）； 架构如下：



第二类属于家电与家庭其他设备联动，如安防、娱乐、门禁等，架构如下图：



## 1.3 IoT芯片/模组接入流程

模块接入流程图如下：

#### 第一步：申请成为合作者

在美的M-Smart开放平台注册账号，成为M-Smart开放平台的开发者。详细步骤请参考开发者注册流程

#### 第二步：商务签约

合作方与智慧家居签订商务合作协议、保密协议等相关工作后，即可往下开发

#### 第三步：厂商适配

开发者需要完成SDK开发，如果对SDK有疑问，美的M-Smart开发平台的工程师可以提供相应的协助。美的M-

Smart平台也会给开发者提供相应的接口说明书，M-Smart协议说明等资料

#### 第四步：厂商自测

开发者开发完成后，需要根据美的M-Smart规范完成相应的测试规范与用例的测试，M-Smart平台将根据已有经 验提供一些测试建议，保证产品质量，保证用户体验

#### 第五步：申请认证

开发者自测完成，没有问题后，就可以提供给相应的模块与测试报告到M-Smart平台审核

#### 第六步：认证资料审核

美的M-Smart平台将对合作者提供的资料先进行审核，模组固件测试前先要确保模组的硬件测试以及射频测试是 已经测试通过的，同时也需要根据模组的规格说明书审核模组测试的功能点与规格书一致

#### 第七步：M-Smart测试

M-Smart平台将针对某些特殊功能做验证，看是否与提供的数据一致

#### 第八步：M-Smart认证通过

M-Smart认证通过后，美的M-Smart平台将提供合格的测试报告，并且在美的M-Smart平台添加合作厂商的名 称与通过的信息，以供大家查询。

## 1.4 IoT芯片/模组接入流程

以下模块已经通过M-Smart认证，可以搭配产品使用!



# 2. 产品接入

## 2.1 产品接入流程

### 2.1.1 M-Smart 产品方案简介

智能家居通过物联网技术将家中的各种设备（如音视频设备、照明系统、窗帘控制、空调控制、安防系统、数字 影院系统、影音服务器、影柜系统、网络家电等）连接到一起，提供家电控制、照明控制、电话远程控制、室内外 遥控、防盗报警、环境监测、暖通控制、红外转发以及可编程定时控制等多种功能和手段。

M-Smart为您提供家居整套解决方案，提供全方位的信息交互功能，甚至为各种能源费用节约资金。

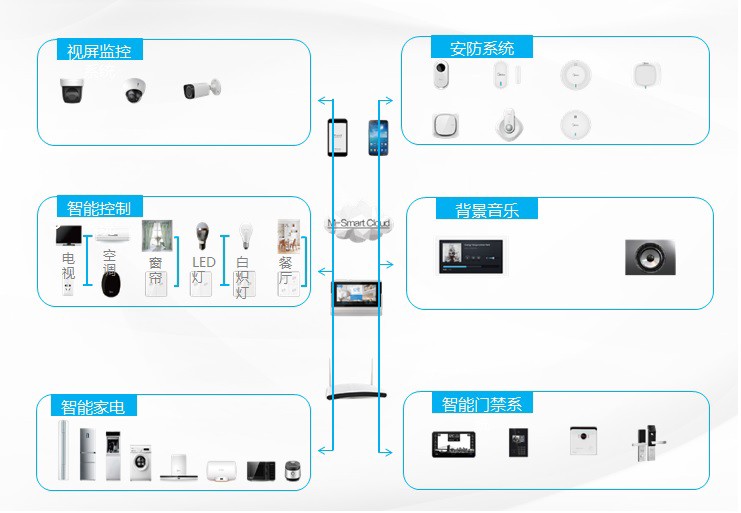
### 2.1.2 M-Smart嵌入式方案集成

产品协作商可以在本站点了解M-Smart方案体系以及接入相关流程。在确认合作意向并签署协议后，可从本站点 开发中心处下载SDK包以及相关技术文档，若是有疑问，可以从联系我们处进行咨询。

### M-Smart产品认证

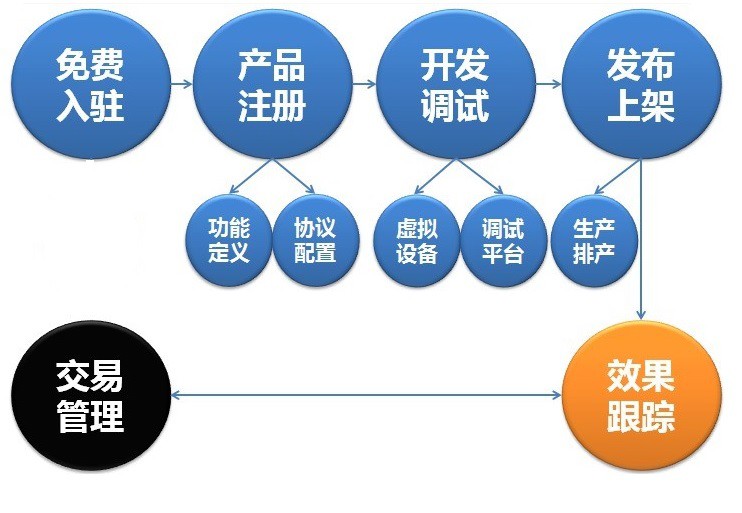
集成M-Smart物联解决方案的产品需要通过相关的认证测试。认证流程由合作商自主发起，美的智慧家居或者第 三方测试机构负责测试验收。通过M-Smart认证测试的芯片及模组方可获得美的颁发的M-Smart认证书，并且可以 在M-Smart官网的成功案例处显示。

### M-Smart产品线



**2.2 产品接入流程**

第一步：申请成为合作者 第二步：商务签约 第三步：厂商适配 第四步：厂商自测

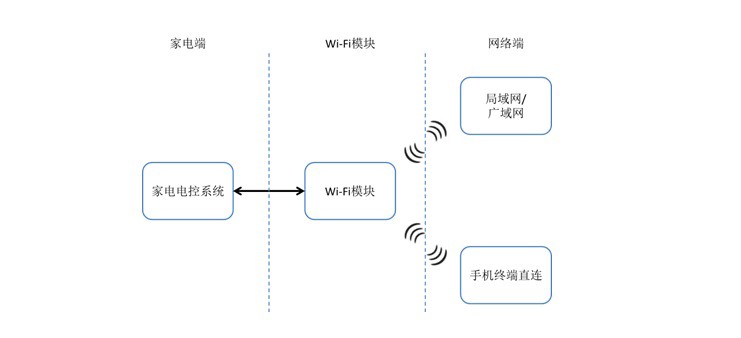
第五步：申请认证 第六步：认证资料审核 第七步：M-Smart测试 第八步：M-Smart认证通过

## 2.3 产品开发调试

### 2.3.1 设备端固件开发

M-Smart智能物联方案对硬件设备数据进行了梳理及定义，智能硬件产生的原始数据需要转化为符合M-Smart协 议格式的智能物联数据。

Wi-Fi模块一方面通过UART通信接口与家电电控系统相连，这一侧称为家电端，或UART端。另一方面，模块通 过无线连接与路由器相连而加入局域网或广域网，也可通过AP直连方式与手机等移动终端连接，这一侧称为网络 端，在不引起歧义的情况下，也称为Wi-Fi端。



### 2.3.2 APP界面开发

The product APP device panel is developed using HTML5 technology and is open to independent development capabilities through the H5 SDK. Manufacturers and developers can follow the design and development specifications of the US APP and develop the APP device control interface to complete the entire process from cloud access, device development, and APP development. The device can be controlled by an APP. Provide a consistent interactive experience and inter-device operations.



### Third Party APP SDK

Worth looking forward to...

### Distribution Network Settings

The distribution network is a necessary step for equipment intelligence, so that the equipment has the ability to connect to the network. The platform currently supports the WIFI network connection mode. Because the distribution network mainly configures the WIFI network, the distribution network includes two steps:

1, distribution network guidance settings: different products, distribution network design is different, especially the product needs to enter the distribution network mode, the difference is very large, need to be set to inform the user.

2, distribution network configuration process: Mercure APP has integrated several distribution network models currently supported, as long as integrated into the Mercure APP, including factory test package and release package, can automatically complete the distribution process, but need to be equipped with network boot settings , that is, distribution network entrance!

### Test recommendations

Based on our experience, we provide the following test recommendations to ensure product quality and ensure user experience. Please pay attention to the quality of the products. If we think there are quality problems, please check the quality of the partners at any time!

#### Test case design principles

* The use case title description is clear and easy to understand, consistent with the use case design content;
* Use case One step corresponds to an expected result as much as possible;
* Expected results are unique and there is no ambiguity;
* If a use case exceeds three steps, it is recommended to split into two or more use cases;
* The use case design does not conflict with the PRD demand point, and the design point is derived from the demand;

#### Test case design recommendations

* APP uplink message control use case:
* Mainly refers to issuing functional commands from the function panel of the APP device. After reaching the device via the cloud, the device can respond correctly and work normally according to the instructions.
* APP downlink message synchronization use case:
* Mainly refers to the function status or data of the APP function panel can be correctly synchronized in time after operating the function command from the device end (mechanical button, touch template, remote control, etc.).
* Functionally exclusive use cases:
* Mainly based on the logic in the functional mutual exclusion table in the provided technical requirements document (TRD), the design functions are mutually exclusive use cases, such as: the air supply is automatic mode, and the wind speed gear position control is not adjustable.
* Function linkage use case:
* Mainly based on the function linkage operation logic in the provided TRD table, design function linkage use cases, such as: set sleep on the air conditioner, then the wind speed will automatically become low wind.
* Report data detection use cases (common use cases):
* Check if the key value of the reported data meets the requirements of the standard protocol specification.
* Message Push:
* Mainly refers to when the device reaches a certain state, one or more messages are sent to the app by the cloud message center. For example, use the oven to bake a food, and when finished, push the message to the app.
* Device affinity function use case:

◦Only support the function of this function, mainly refers to the appointment timing function use case design, device scene function use case design, only need to design the most basic use case.

* Network usage scenario use case (common use case):

◦3G, 4G and other network control operations 控制WIFI network control operation

◦3G switch WIFI, WIFI switch 3G control operation

* Copywriting, visual, adaptation test cases (common use cases):

◦Writing case description, whether the prompt is simple and easy to understand

◦The control layout and adaptation are consistent with the PRD. There is no visual design that affects the experience.

* Fit the phone, the test is based on the phone in the compatible phone list.
* Distribution network:
* Distribution network delay (not more than 20s)
* Distribution network success rate

多次Multiple continuous distribution of the same device

二Two devices of the same model are respectively equipped with network binding

◦The device triggers the distribution network mode (for example, if you press N times consecutively to enter the distribution network, what will happen if you continuously connect N+1 times)

* Untie

◦APP unbind device validity

* Device hardware (such as reset) operation, clear the binding relationship of this device with all accounts.
* Other use cases (common use cases):
* Power on for a long time (>12 hours), whether the control device is in effect.

## 2.4 effect tracking

Integrate device users, user data, behavioral data, industry data, and peripheral data through the cloud platform big data collection platform, and based on this, support multi-dimensional device usage and user behavior data analysis. Data helps you better analyze the use of users and devices to better plan and design products and marketing strategies.

Data report

Provide real-time reporting capabilities to device vendors and developers. Including user growth, equipment growth, by category, by model, by region; Provide user operation behavior analysis statistics.

Example:







# Contact information

M-Smart hardware development contact: [weishan.lu@midea.com (mailto:weishan.lu@midea.com)](mailto:weishan.lu@midea.com) M-Smart hardware certification contact: [yali.liu@midea.com (mailto:yali.liu@midea.com)](mailto:yali.liu@midea.com)

M-Smart Product Development Contact: [pan.wang@midea.com (mailto:pan.wang@midea.com)](mailto:pan.wang@midea.com)

[M-Smart product certification contact: zhaozhong.deng@midea.com (mailto:zhaozhong.deng@midea.com)](mailto:zhaozhong.deng@midea.com)

Appendix C: Email to Instant Pot Privacy Office



**Questions Regarding Privacy and Data Collection**

1 message

**Rick Givens** [**<rpgivens@gmail.com>**](mailto:rpgivens@gmail.com)

**Rick Givens** [<rpgivens@gmail.com>](mailto:rpgivens@gmail.com) Sat, Jul 6, 2019 at 4:02 PM To: [Privacy@instantpot.com](mailto:Privacy@instantpot.com)

Hello,

I am an owner of an Instant Pot Smart Wifi Pressure Cooker, and I have several questions/concerns regarding the device, its data collection, and the control app. This is part of research which will be published in a thesis by the end of August.

Please provide detail regarding the items below.

I decompiled the .APK file and examined the code for the control app; I see that you are using Sentry for error reporting (snippet from main):

u.init({

dsn: "<https://90b2669b810f432aadfaa44fde88e9e9@sentry.io/145987>", release: n.commit,

attachStacktrace: !0, beforeSend: function(e) {

if (!l.shouldSend(n, e)) return null;

var t = e.stacktrace || e.exception && e.exception.values[0].stacktrace; return t && t.frames.forEach(function(n) {

n.filename = n.filename.substring(n.filename.lastIndexOf("/"))

}), e

I can see from the logs in my phone's filesystem that you obscure my identity when error reports are sent:

2019-06-20 20:31:33.144 (SLK: :[MSmartUserManagerProxy.loginWithAccount(Line:119)]) loginWithAccount: [user-622960.45e109dddc@msmart.instantpot.com](mailto:user-622960.45e109dddc@msmart.instantpot.com)

However, further down the log is this:

2019-06-20 20:31:33.845 (SLK: :[fg$a.a(Line:409)]) Request:<https://mapp.appsmb.com/v1/user/info/get> I 2019-06-20 20:31:33.845 (SLK: :[fg$a.a(Line:410)]) Response: [code: 200 message: OK response:

{"msg":"ok","result":{"uid":"","address":"","profilePicUrl":"","phone":"","registerTime":"2019-06-03

01:05:04","signature":"","sex":"","nickname":"[user-622960.45e109dddc@msmart.instantpot.com](mailto:user-622960.45e109dddc@msmart.instantpot.com)","mobile":"","id":" 1593940","email":"[user-622960.45e109dddc@msmart.instantpot.com](mailto:user-622960.45e109dddc@msmart.instantpot.com)","age":""},"errorCode":"0"}]

As I see there are fields for personal data, I wish to know if any of this (sex, nickname, age, etc) is captured. Though it does appear to be blank, I wish you to confirm this.

Furthermore, Sentry states on their website documentation that sensitive data may be sent as part of issue notifications [(https://docs.sentry.io/data-management/sensitive-data/), that it allows data forwarding (https://docs.sentry.io/data- management/data-forwarding/), and that it supports additional context with events, including Unstructured Extra](https://docs.sentry.io/data-management/data-forwarding/) Data [which is described as "Arbitrary unstructured data which is stored with an even sample". (https://docs.sentry.io/enriching- error-data/context/?platform=javascript).](https://docs.sentry.io/enriching-error-data/context/?platform=javascript)

What is the nature of the sensitive or arbitrary data that is collected, how is it stored? In what ways is it secured?

Also, you state on your privacy statement "We store your personal data in Canada and with AWS under the highest data security standards. AWS is certified under the EU-US Privacy Shield." However the server [mapp.appsmb.com](http://mapp.appsmb.com/) is registered in China, and appears to be affiliated with Alibaba and Midea (who provided the SDK for the app and manufactured the wireless card in the control board). <https://www.mydomain.com/whois/whois.bml>

As EU US Privacy Shield deals with data exchange between the US and the EU, please explain to me what safeguards are in place with the appsmb server.

As Midea provided the wifi module and the SDK, does the device communicate with the Midea Cloud Service (<http://iot.midea.com/>). Under the M-Smart Certification Platform Overview, 2.4 Effect Tracking, it is stated (per

translation):

Integrate device users, user data, behavioral data, industry data, and peripheral data through the cloud platform big data collection platform, and based on this, support multi-dimensional device usage and user behavior data analysis. Data helps you better analyze the use of users and devices to better plan and design products and marketing strategies.

Data report

Provide real-time reporting capabilities to device vendors and developers. Including user growth, equipment growth, by category, by model, by region;

Provide user operation behavior analysis statistics. <http://iot.midea.com/develop/docshow/auth#item-330>

What specific analysis are you collecting or have enabled in your platform? What user behavior analysis are you conducting, and what data is included?

Finally, I see that the control app uses the Apache Cordova module. Several of the plugins make sense, such as the need to access location, and wifiwizard2. However, I fail to see the need for the following plugins: socialsharing, printer,

camera, and filetransfer. What is the purpose behind having these cordova plugins as part of the .APK file? What functionality is enabled? Does the InstantPot app access any portion of phone storage, contacts, camera, or transfer files for any reason and if so, why?