IoT in Smart Homes: Security and Privacy by Design

Leah Goggin
MIT

Mine Kansu
MIT

Alice Lee
MIT

Benny Tang
MIT, Akamai

December 8, 2018

Abstract

The proliferation of internet connected devices is an opportunity to bring convenience and efficiency to existing consumer devices and to create entirely new categories of devices. These changes are not the result of merely better hardware and software but of the inherent value of network effects. These network effects also bring new threats that must be addressed by a combination of technical and policy measures. We recommend technical changes that can be implemented by communications standards such as Zigbee to ensure higher security and privacy for users of home IoT devices.

Executive Summary

This white paper addresses some of the existing privacy and security threats in the fast expanding use of Internet of things (IoT) devices in smart homes. The paper: (i) provides an analysis of the policy and threat landscape for home IoT; (ii) assesses the technical devices and protocols in use (the Zigbee protocol as a key case study); (iii) makes recommendations to improve the existing technical standards.

The industry is growing quickly in terms of both the number of devices installed and the number of new systems available. These devices collect a significant amount of data that are deemed private or sensitive by their users. As the network of connected devices increases through different media and industries, IoT systems expose their users to privacy and security challenges that can lead to leaks of sensitive personal information, physical threats, and significant cyber attacks.

We chose to focus on home automation as it is likely to be familiar to the reader, is one of the largest subsectors of IoT, and is currently governed by few laws (unlike connected medical devices). The users in this segment are mostly individual consumers with limited technical knowledge and limited means of protecting themselves. Companies attempt to design simple, user-friendly devices there are usually installed by the consumers themselves.

Home IoT systems collect a significant amount of sensitive data on users, putting individual consumers at significant risk. The privacy and security threats become more significant when multiple connected devices are compromised since data integration leads to more accurate insights about devices users, which increases their exposure to privacy and security risks.

This paper is aimed at protocol designers and technical consortium members who play an important role in designing and standardizing IoT protocols. These protocol specifications and associated hardware parts and software libraries are leveraged by IoT device manufacturers and developers when building IoT devices and products.

In order to identify strengths and weaknesses in the current home IoT security and privacy protocols, we examined the Zigbee protocol as a case study. Zigbee provides one of the most widely used specifications for IoT communication. We also include a brief discussion about the genuine value that networking devices can bring to the consumer.

Using a high-level threat model—an analysis of what assets are in play, what defenses are in place, and who is trying to compromise them and how—we reason that adversaries are who are motivated by some combination of money and notoriety are the most likely attackers. Considering no device can be fully secured against an adversary with unlimited resources and time to execute an attack, this scoping is essential to our recommendations. Realistic adversaries are defined by their likely resources, system access, risk tolerance, and objectives.

We also examined the policy landscape by looking at the rules that govern device security and data security. Our focus is on recent and upcoming regulations and policies in the US and EU, the governmental entities at the forefront of IoT regulation. This review helped us identify the areas which policy makers have yet to address in order to evaluate whether any of these areas can be tackled with technical solutions.

Before presenting our analysis, we have categorized the key concepts identified in our analysis into a maturity scale. We recognize that most of our recommendations are well known within the security community, but the average developer is unlikely to be aware of the techniques we discuss. For this reason we propose integration approaches that would move the burden of security from individual devices to the shared protocol. As a result of our assessment of the Zigbee protocol, we identify the key measures that can be addressed through a technical solution as: password requirements, software updates, and dangerous actions like pairing "failing closed."[1] We also include recommendations for design-level security techniques that can be prompted by changes to the protocol.

[1] Rather than accepting errors, put the device in a safe mode.

Contents

1 Introduction

1.1 test

Hello world.

2 Communication Protocols and Standards

While digitally controlled home appliances have existed for decades, allowing those devices to communicate with each other and the company that built them is a new phenomenon. There are many benefits to such communication, including more frequent software updates and energy savings, but a downside is that the introduction of thousands of devices of the same kind, often with the same vulnerabilities, makes consumer products a tempting target for attackers. Furthermore, IoT devices have limitations on processing and battery life that arent present for the typical desktop computer or even the typical smartphone.

It is important to differentiate between**standards** and**protocols**. A communications standard is a set of guidlines that a group has agreed to follow, while a communications protocol defines exactly how data is exchanged and the expected behavior. Agreeing on a standard is like agreeing on a language to speak in are agreeing to a protocol is like agreeing to a script to read.

One of the most common standards for developers who are not interested in creating bespoke solutions is Zigbee.

2.1 Case Study: Zigbee PRO

Zigbee is an IEEE 802.15.4-based specification for self-organizing, wireless adhoc networks. Zigbee has three main offerings: Zigbee IP, Zigbee RF4CE, Zigbee PRO. This paper focuses on Zigbee PRO because the owners choose to open source most of the information and is widely used in home automation applications.[2] Zigbee PRO provides the most options to users and is considered the most current of the three main Zigbee offerings.

The Zigbee specification is made up of abstractions layers: an application running on a device only needs to see the content delivered, not exactly the frequency the radio is running on. More specifically, there are three layers in the specification: application, network, and security. Each layer is designed to be as generalizable as possible so that the code can be reused as much as possible so that developers don't have to solve the same problems (with incomplete messages, say) every time a new project is started. Zigbee standards designers are thus incentivized to choose to create tools that are useful to everyone in order to provide functionality while keeping the standard easy to understand. This instinct is often a very good thing when it comes to non-security problems like message passing, as it gives a developer a lot of power to make new devices and the security of knowing that future devices are likely to be able to network

[2] See appendix.

using the same standard. An inexperienced developer therefore has a lot of power to design different products, but not a lot of guidance on designing those products in a secure way.

When it comes to building secure devices the security layer delivers all the basic tools an expert would need to build a device designed for security and privacy. The choice to provide such fundamental mechanisms—specifcially, cryptography "primitives" like encryption and authentication—is in keeping with the goal of a design that is as general as possible. However, those operations (assuming they're even used in the first place) can be miused to the point of uselessness. An insecure password or, worse, a password that is announced to the whole world will not provide confidentiality if used for encryption. Secure algorithms are difficult to design and implement correctly, so the developer should be provided with protocols that handle common operations like two devices communicating confidentially.

2.1.1 The Zigbee Control Network

A Zigbee network consists of devices, or nodes. Every node is defined by the presence of a microcontroller, transceiver, and antenna. Nodes operate as either full-function devices (FFD) or reduced-function devices (RFD) - the former is capable of performing all tasks as defined by the Zigbee protocol, while the latter only performs a limited, defined number of tasks that is often a subset of the Zigbee protocol. Nodes can be categorized as follows (Elahi & Gschwender, 2009):

- **Coordinator:** An FFD that is responsible for overall network management of the Zigbee network, including starting the networking, assigning addresses, controls joining/leaving of other nodes, and transfers application-layer packets. Every Zigbee network has exactly one coordinator.

- **End Device:** Often an RFD, which enables it to consume less power, and frequently only consumes power while transmitting information.

- **Router:** An FFD, used in both tree and mesh topologies to expand Zigbee network coverage, as well as find the fastest route from device to device to transmit information.

- **Zigbee Trust Center:** A device that provides security management, security key distribution, and device authentication. This is frequently the coordinator device, and exists as exactly one device in each network (Rudresh, 2017).

- **Zigbee Gateway:** The gateway, often the same device as the coordinator or a router, is used to connect the Zigbee network to another network, such as LAN, by performing protocol conversion.

This architecture is important as it operates mostly invisible to the users, meaning that users typically do not need to establish the role that each device plays. Its an important first step as it allows certain devices to be built deliberately more secure in order to operate as a Zigbee Trust Center, and centralize critical operations such as authentication.

3 Threat Model

As identified previously, the introduction of commercial IoT devices into the home presents a threat to the users information security and privacy. The use of a threat model allows the identification of possible attackers and an assessment of which attacks are the most likely—in this case, the attackers with whom we are concerned from a technical perspective are financially motivated, rather than personally or politically, and likely to only pursue attacks that are high-paying or automatable. This evaluation will allow the identification of not only shortfalls in the technical and policy measures, but also places where attempts at security may have overshot the optimal tradeoff between security and efficiency, usability, etc.

This section will analyze the security context of home automation in general using Salter et. al.s three-step process:

1. Modeling the resources, access, risk tolerance, and objectives of adversaries, noting that the defender might value an asset completely differently than the attacker (Salter et. al., 2)

2. Modeling the vulnerabilities of the system and the corresponding countermeasures, taking into account the life cycle of all components

3. Synthesizing knowledge about the system and potential attackers to design the most rational countermeasures

3.1 Adversaries

We assume that financially-motivated cybercriminals who do not personally know the victim are the most relevant threat in the context of home automation that can potentially be addressed with technical or regulatory solutions (please see Appendix for further information on different types of adversaries and justification of this conclusion). It is then possible to identify the adversaries resources, access, risk tolerance, and objectives as Salter et. al. recommend.

- **Resources:** Salter et. al. characterize criminal hackers resources as moderate. An organized crime ring may have many skilled attackers solving the same problem (but only as many as the expected payoff makes rational). They may have anonymous bulletproof hosting resources, a repository of developed-in-house malware, etc. They will generally not have the level of funding and computational resources of a nation-state actor.

- **Access:** It is unlikely that a cybercriminal has any special access to Internet infrastructure, corporate data, etc. They may have any leaked information such as source code that is available on the clear web, on hacker forums, etc.
- **Risk Tolerance:** Cybercriminals are strongly incentivized not to get caught if there is the possibility of arrest. However, an important consideration is that commercially-motivated cybercriminals are often operating internationally, and often from countries in which prosecution is unlikely. In several countries from which a large portion of cybercrime originates, such as China and Russia, there is an unofficial detente between hackers and the government, the understanding that hackers may operate more or less with impunity as long as all costs are imposed outside the countrys borders (DeSombre).
- **Objectives:** Attackers may monetize access to home automation devices through roughly two assets: personal information (including credentials and financial information) and the ability to execute code on the device. We assume that the attackers objective is getting one or both of these assets.

There is the possibility of an attacker who does not know the victim personally nonetheless wanting access to non-monetizable data, such as the feed from IP cameras. For threat modeling purposes, this will be considered to be part of the attacker after sensitive personal data case.

This threat model is crafted from the perspective of the manufacturer. It should be noted that the consumers threat model may differ slightly. While the manufacturers and consumers intentions are generally aligned with respect to keep data and resources away from cybercriminals, the consumer must also concern themselves with the possibility of personal data being sent to the manufacturer in a way that may be the manufacturers attention, and even disclosed to the consumer, but which the consumer does not wish to transmit.

3.2 Vulnerabilities

The vulnerabilities relevant to home automation are discussed in the Security and Privacy Threats for Smart Homes section above. Some examples of Zigbee-specific vulnerabilities and exploits are described in the Appendix.

3.3 Synthesis

As Herley observes, it cannot be the case that every one of the several billion Internet users worldwide is constantly being attacked by a skilled adversary targeting them personally; there are simply not enough such skilled adversaries to go around (Herley, 2014). Since the focus has narrowed to financially-motivated cyber criminals as their attention can be expected to go wherever there is the most potential for a payoff, with some adjustment for risk (e.g. hackers preferring to operate outside their own country). The odds of exploitation can therefore be greatly lowered with even a modest investment in security, if that investment is targeted such that exploitation of a device, while it may still be technically possible, is simply not worth an attackers time. Herley captures this succinctly: the defense effort should be appropriate to the assets (Herley, 66).

The attacks related to data privacy may offer a significant payout per device exploited, due to the possibility of subsequent fraud or extortion. Attacks on device security for the purpose of stealing resources rely more on scale—an attacker must be able to exploit many devices relatively easily for the attack to be worth the time. An exploit requiring the attackers personal attention on each device is therefore unlikely to be pursued; instead, the attacker will focus on exploits that can be automated and deployed against many devices at once.

A rational security posture for a home automation device, then, is one which (i) closely guards information that can be directly and easily exploited for a significant payout, and (ii.) resists automated attempts to inject code.

4 Policy Landscape

In addition to efforts of technical consortia such as Zigbee, policy makers have also been paying attention to privacy and security issues related to new technologies. From a policy perspective, data security and device security are usually treated as separate issues. Some legislative efforts and policy frameworks are emerging in Europe and the US, but these efforts seem to be still in the early stages. The recent policy efforts have largely focused on the needs of the more mature online ecosystems such as social media platforms. Recently, the newer technologies such as IoT are also gaining attention as these technologies are being utilized in security sensitive settings (such as healthcare or government use).

The purpose of this section is to identify the current regulatory efforts that shape the policy landscape for IoT development. We identified the crucial concepts in IoT security and privacy that we believe can be addressed by policy, and assessed the selected list of regulations in regards to these concepts. This assessment helps identify the areas in which the technical standards can help close the security and privacy gaps vs. the areas where there is need for regulations or new policies to strengthen the IoT ecosystem.

4.1 Review of Existing Policies

We restricted our review of the major IoT related privacy and security regulations and standards to those in the US and the EU as these countries tend to share similar values in privacy and have been the leaders in technology regulation. The following table shows the the key principles of device and data security that are addressed in major regulations from these regions that are applicable to home IoT:

Note that the documents marked with * are still in draft form. The IOT Consumer TIPS Act of 2017 and IoT Cybersecurity Improvement Act of 2017 have been introduced, but they await a long process until they pass both the Senate and the House and become a law, and the text may change significantly during the process. For the purposes of our analysis we treated these bills as law of the land in the US, with the assumption that any future law to be implemented by the US government will be largely similar to the present version of these bills.

The range of coverage of these documents vary significantly. While GDPR targets data protection directly, others like the IoT Cybersecurity Improvement Act only focuses on device security questions. The UKs Code of Practice for IoT Security stands out in the list as the most comprehensive guidelines covering a wide range of topics addressed to many different stakeholders in the IoT ecosystem, but it is currently only a list of recommendations with no liability enforcement on IoT providers.

Looking at the safety and privacy concepts being covered in these policy documents, we observe that some of the concepts such as the right to be forgotten and vulnerability notification are better understood and are addressed by policy makers, while other newer concepts that are more relevant to newer technologies such as IoT are discussed in some or none of the documents. Further discussion of each concept is provided in the next section.

5 Analysis and Recommendations

6 Conclusion

Appendix