Research Paper Summary

Shaolun Liu, Kaiyu Dong, Long Chen

Simon Fraser University
{shaolun_liu,kaiyu_dong,long_chen_3}@sfu.ca

Keywords: IoT device · Security.

1 Rethinking Access Control and Authentication for the Home Internet of Things (IoT)

1.1 introduction

Nowadays, multiple users are not uncommon to interact with a single device. Based on a study of 425 participants, the access-control policies for different capabilities on a single device are in high demand. As a result, more and more IoT home devices are deployed for consumers, such as Samsung SmartThings, the Amazon Echo Voice assistant, the Nest Thermostat, Belkin's Wemo devices, and Philips Hue lights. Meanwhile, little attention and effort have been put onto access-control-policy specifications, which is surprisingly unexpected. Therefore, it is necessary to rethink the access control and authentication of IoT devices which are distinct from traditional appliances such as cell phones, computers, and tablets, that usually can only be used by a single person. It means IoT devices require more specifications in authentications and access control since they may be used for different functions by different users.

1.2 background

Home IoT devices are different from traditional devices, and many users may interact with a single device with specific characteristics. For instance, the household's voice assistant and internet-connected door lock may have wide accessibilities compared to children, guests, and other family members on the property. Many home IoT devices do not have a screen or even a keyboard for users to input their username and password for authentication purposes. It will make it more challenging to set different specifications based on the identifications of the users. One of the solutions would be using their phone as a central authentication mechanism. In this context, small Internet-connected appliances or devices used in the home are primarily considered home IoT devices.
Here are some Research Questions included in this article:

1) Do desired access-control policies differ among the capabilities of single-home IoT devices?

2) For which pairs of relationships (e.g., child) and capabilities (e.g., turn on lights) are desired access-control policies consistent across participants? These can be default settings
3) On what contextual factors (e.g., location) do access-control policies depend?
4) What types of authentication methods balance convenience and security, holding the potential to balance the consequences of falsely allowing and denying access successfully?

In this article, the main proposed contributions are listed as follows:

· Proposing access-control specifications for the multi-user home IoT based on capabilities that better fit users' expectations than current approaches.
* They show the frequent context-dependence of access-control policies, identifying numerous contextual factors that future interfaces should support.
* It is setting an agenda for authentication in the home IoT based on methods that minimize the consequences of falsely allowing or denying access.

Two significant challenges are parties that have physical access to the home and those external third parties, including those who exploit vulnerabilities in the platform, devices, or protocols intending to cause damages physically, financially or privacy related. Those with physical access to the home include household members with legitimate access to the home, such as temporary workers or children.
A list of home IoT devices from consumer recommendations in CNET, PCMag, and Tom's Guide is generated from the pre-study:

1.3 Categorization

There are 24 relationships based on the study of participants. (e.g., teenage child, home health aid), then categorize them into six relationships (spouse, teenage child, child in elementary school, visiting family member, babysitter, neighbor) that span the range of desired access and are also consistent to participants. Let the participants choose from "always," "sometimes," and "never" for each accessibility. The survey is conducted online and focused on workers that are 18+ in age and living in the United States to elicit the policies of the desired access-control,

1.4 Access-control policies

Research Question 1:
It is observed that participants' attitudes towards various capabilities will differ even within a single device. for instance, participants are more willing to let others to play music (32.5% of participants choose never averaged across the six relationships, $\sigma = 0.33$, median = 23.7%) than other order things online (59.7 % choose never on average, $\sigma = 0.40$, median = 71.1%). Relationships also play an important role in participants' preferred access-control policies. For instance, babysitters would be granted permission at a higher rate than visiting family

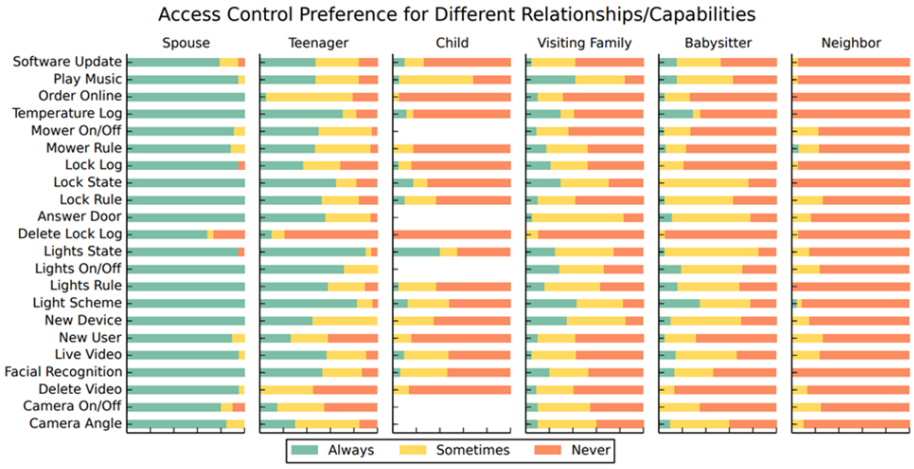

Fig. 1. Participants' desired access-control policies. We introduced participants to a list of relationships (e.g., neighbor) and asked them to choose whether someone in that relationship should be permitted to "always," "sometimes," or "never" control a capability (e.g., adjust the camera angle) in their smart home.

members. 57.1% of participants decided that a visiting family member would never have access to the features such as "Live Video," while only 33.3% of participants decided the same for a babysitter. It becomes achievable on access-control IoT devices compared to single-access home IoT devices.
Research Question 2:
Based on the study, the primary capability for which age played less of a role was changing the camera angle. Many participants were concerned with letting a young person access specific capabilities. Device locations are the second most frequently invoked factor for turning a camera on or off (60%) and watching a live video (81%). 51.7% of participants agreed that recent usage history impacted their decision about access-control policy. one participant wrote, "if someone were to misuse the device, you best bet they are not getting a second chance." The time of day, location of a user, costs, people nearby and state of the device are also important parameters affecting participants' decisions in the access-control policy.

1.5 Conclusion

The user study shows that a capability & relationship-centric model more closely fits users' expectations. Home IoT technologies would allow achieving it through different methods, such as that one user can increase the lightness of the room by voice assistant and the other user may decrease it through the smartphone. The article also discussed authentication mechanisms and commented on their ability to identify users, relationships, and contextual factors.

2 Looking from the Mirror: Evaluating IoT Device Security through Mobile Companion Apps

2.1 Introduction

Smart home IoT devices are chosen by attackers due to user ignorance and poor security design. As attackers' motivations develop (IoT botnets, personal data theft), smart home security incidents will rise. This is a multifaceted challenge. First, many of these vendors are tiny and medium-sized firms without the money for software quality control and security best practises, resulting in vulnerable devices. Second, many of these devices are cheap (typically less than $100) and cannot afford sophisticated security infrastructure like monitoring agents, encryption and authentication hardware, etc. When a gadget is susceptible, the vendor has little motive or capacity to offer a repair. Third, vendor fragmentation makes patch management and distribution difficult.
Identify vulnerable devices before deployment and protect them. Upgrade the device's firmware, prohibit traffic that potentially exploit the vulnerability, or quarantine the device. Multiple ways have been presented to identify vulnerable devices. One line of research launched an Internet-scale scan to find publicly accessible devices with weak passwords, certificates, and keys. These approaches can't identify devices with sophisticated vulnerabilities or those concealed behind NAT. Another line of research analysed IoT devices or firmware statically and/or dynamically for security. These methodologies give more complete and precise data for individual devices, but not for large-scale study. First, obtaining physical access to all gadgets on the market isn't possible due to limited availability in some locations and expensive purchase costs. Due to the market's fragmentation, device firmware is not always available. Second, even with a device or its firmware, analysis is typically tedious, error-prone, and complex, especially given the "device shell" device sellers often put in place (e.g., packing, obfuscation and encryption). The market would benefit from a method that quickly identifies vulnerable devices and narrows analysis scope.

2.2 System Design

This study presents a technology that accelerates vulnerable device detection and analysis without physical or firmware access. Two observations guide our approach. Small and medium-sized smart home IoT device producers commonly use the same components (e.g., software from open source projects, hardware from common suppliers) to develop their devices. Therefore, IoT devices often share the same vulnerabilities or poor security procedures. By comparing an unknown device to vulnerable ones, we may spread vulnerability information. Second, mobile companion applications represent device commonalities. Combining these two discoveries allows us to design a platform that finds vulnerable devices without the actual devices or firmware images.

Fig. 2 shows our platform. The IoT App Database stores smart home IoT device companion apps scraped from Google Play. The app database is continually updated (e.g., when new IoT devices are on market or old apps get updated). App Analysis Engine analyses IoT App Database apps. The App Analysis Engine analyses code to estimate an IoT device's characteristics. The App Analysis Engine computes a device's network interfaces, imprints, and code signature. App Analysis Database stores Engine's results.
A Cross-App Analysis Engine queries the App Analysis Database to generate a device family. Device families group comparable devices from different vendors. Similarity in different dimensions (e.g., similar software, similar hardware, similar protocols, and similar cloud back-end services). The gadget family allows vulnerability information to spread. It evaluates IoT device security from a device or threat standpoint. 1) For a specific device, similarity allows quick assessment of susceptibility and, if so, to which vulnerabilities; 2) For a certain vulnerability, determine the list of market-available devices that may be affected. Our platform includes Device Firmware Collector to confirm vulnerabilities. It uses code analysis results (e.g., Firmware URLs) and Internet search results to download firmware images into a Device Firmware Database. These firmware images let us confirm Cross-App Analysis Engine vulnerabilities. Our platform does not require the Device Firmware Collector. It's used to confirm platform findings.

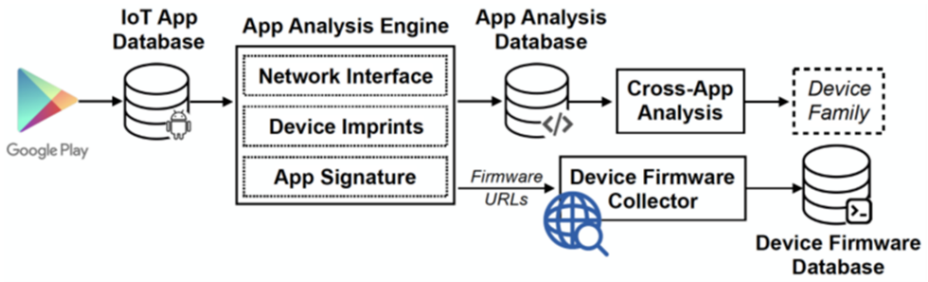

Fig. 2. Platform overview

2.3 Results

We downloaded 3,094 IoT companion apps from Google Play for our testing. We had 2,081 apps after removing noise. Our platform evaluated these apps.
First, we found device clusters, or device families, with similar software or hardware components, back-end services, and network protocols. In our investigation, we uncovered 19 device families that shared software components across 139 apps from 122 vendors. 48 families comprising 460 devices shared comparable back-end services.

Second, we used the identified device families to identify vulnerable devices. In one case, we discovered devices from four different vendors (whose apps are used by more than 215,000 users) that were previously unknown to be vulnerable to a software vulnerability and independently confirmed the vulnerability on 45 devices from four different vendors that were previously confirmed by other sources. We identified 67 devices from 16 vendors with a hardware security problem. Our platform found 324 susceptible devices from 73 vendors. During validation, we could decide on 179 devices from 43 vendors, of which 164 (91.6%) are vulnerable.

2.4 Conclusion

We provide a platform to speed up smart home IoT device vulnerability discovery. Our software analyses mobile companion apps to detect device similarities and vulnerability propagation across devices, making it suitable for large-scale analysis. By analyzing 2,081 mobile companion apps, our platform found 324 devices from 73 vendors that are potentially exposed to security concerns; 164 devices from 38 suppliers are proven to be vulnerable.

3 Medical Device Security in the IoT Age

3.1 Introduction

In the United States alone, the Medical Device market size has reached $133 billion with over 6,500 medical device companies in the US alone. The greatest danger in a mass attack probably lies in an attack on the availability or integrity of medical devices. Such an attack could lead to delayed care, an inappropriate diagnosis, or the potential loss of protected health information.
Device manufacturers are increasingly concerned with the functionality of the device and not the security of the software. In the worst-case scenario, a compromise in availability or integrity could result in the loss of life. There is a lack of regulations around medical device manufacturers and the responsibility of those manufacturers to take a security-minded approach. The FDA concerns itself only with cyber issues that cause a loss of life. Since devices are primarily developed to save lives and improve healthcare options, security becomes an afterthought.

3.2 Problem Formulation

Health care organizations must decide to mitigate the risk as best they can without a significant regulatory change that may take years. The fix to the problem must be a multi-echeloned approach that balances safety with security while working proactively to request regulatory changes that will allow devices to be safely upgraded.

3.3 Analysis

There is a consensus that proactive steps need to be taken to protect information and networks from the vulnerabilities that are inherent in most connected medical devices. Until manufacturers begin to design devices with cyber security best practices in mind, the healthcare community will need to take action to first understand the risk and second mitigate that risk.

3.4 Inventories

Most health care organizations will first need to identify the devices that may pose an issue to their network or patient safety. This may seem like a relatively simple task, but it is a monumental task. Traditional IT scanning tools are not 100% effective due to issues with the use of antiquated software or MAC addresses that do not correctly map to a specific product.
A full inventory of a health care organization's medical devices will need to take a robust approach that uses a wide net to capture the necessary information from connected medical devices. This would need to be an asset management tool with enterprise capabilities that can capture and reflect multiple fields critical in identifying vulnerabilities and risks.

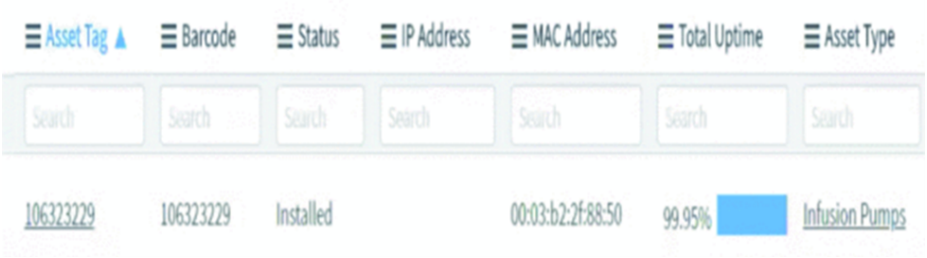

Fig. 3. Diagram of the medical device asset record

Health care organizations need to be able to accurately state what connected devices they have and what the potential vulnerabilities and risks each connected device may pose are. This is an arduous undertaking, so a flexible system must be in place to record the updated information.

3.5 Developing a System of Record

A single system of truth will allow healthcare organizations to better understand the risks associated with connected medical devices on their network. The chosen system must maintain flexibility and data cleanliness to ensure that duplicates and other types of data issues are avoided for the data to be trusted by management and security teams.

3.6 Vulnerabilities and Gaps

Software needs to be identified in all connected medical devices so that IT understands the vulnerabilities of each connected device. Critical information on these devices can be stored in the system of record. Some devices may already have the ability to be patched because the patch has been approved by the FDA. Security professionals can take immediate steps to upgrade the security posture of some connected medical devices by simply understanding the vulnerabilities. With respect to those devices that may have vulnerabilities that do not have a current patch in place, organizations will now have the context to make appropriate risk based decisions.
The basic steps outlined above are not a perfect solution, but until regulatory changes happen or manufacturers become more security-minded in the medical device design phase, they are appropriate. This type of data reporting will allow healthcare organizations to make better decisions on current medical devices and future purchasing decisions.

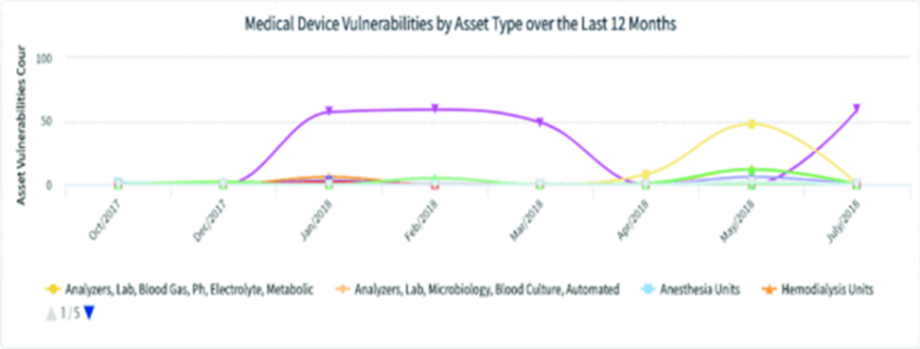

Fig. 4. Diagram of medical device vulnerabilities

3.7 Proposed Changes to FDA Process

The FDA needs to take a more proactive security approach to medical device approval. There will still be a large number of legacy devices in the middle of their device lifecycle. Health care organizations will continue to need a process that will help them to identify, access, and maintain devices that are not easily identifiable.
The minimum recommendations proposed in this paper center around three items:

1) Forcing device manufacturers to take a security-based design approach to device development.

2) Taking significantly quicker action in approving modifications to devices to patch known vulnerabilities.
3) Increased data-sharing between manufacturers and health care organizations to better track equipment and potential deficiencies; including fully building out the unique device identification system.

3.8 Way Foward

This paper aims to help provide effective ways for healthcare organizations to effectively understand the risks associated with their medical device inventory. In the future, the focus will be on showing the results of a full scan of a health care system; providing full results of the medical devices captured and associated vulnerabilities.

3.9 Conclusion

The risk to the availability and integrity of medical devices is real. A single system of record is necessary to understand what connected devices an organization utilizes as a part of patient care. Technology continues to move at lightning speed, and security and safety are critical. It would be a true tragedy if these same life-saving devices, due to a security incident, ultimately resulted in death.

4 Summary

4.1 Current Problem

The issue has arisen as technological gains have significantly increased the connectedness of medical devices. Additionally, medical devices are using disparate software, and medical device manufacturers concern themselves more with the functionality of the device and not with the security of the software. In the worst-case scenario, a compromise in availability or integrity could result in the loss of life.

4.2 Temporary Solutions

Conducting a full inventory of a health care organization's medical devices. The approach to this inventory will require a system of record to capture the medical devices.
Also, the study shows the access-control policies may differ among devices, relationships with the homeowners and authentication methods. It allows the system to learn from the mistakes such as falsely denying and falsely allowing once it occurs. It is time for operators to focus on the access-control policy design and bring appliances into the IoT era. For instance, in different hospital departments, the relationship to the devices can be categorized into identifications of the

users, such as "Cardiologists", "Surgeons", "Medicine Specialists", "Emergency Medicine Specialists", "Administration Staff", "Security", "Nurse", "Check-ups Patient", "Emergency Patient". As mentioned in the final conclusion, accessibility, such as lock status, functionalities of devices, light scheme, entertainment devices and different medical equipment, first aid equipment and administration log, can be categorized into "Fully Accessible", "Accessible with Permission", and "Accessible with restricted time or duration".
According to the report of SonicWall, there was a 123% increase in IoT malware attack volume in healthcare last year. In order to prevent medical devices from being attacked, hospitals can use across-app analysis, which was mentioned previously, to identify whether there are some vulnerabilities in the machines. Because the price of medical equipment is usually high, and once attacked, the consequences are relatively more serious. This method of using only the mobile app without actual devices can be very helpful for hospitals to easily know the safety performance of the devices when purchasing new medical devices, which saves unnecessary costs for hospitals.

4.3 Proposed Changes to FDA Process

Forcing device manufacturers to take a security-based design approach to device development.
Taking significantly quicker action in approving modifications to devices in order to patch known vulnerabilities.
Increased data-sharing between manufacturers and health care organizations in order to better track equipment and potential deficiencies; including fully building out the unique device identification system.