Information Assurance & Security (CSE 543) MCS Portfolio Report

Chirag Bhansali
Arizona State University
Tempe, US
cbhansal@asu.edu

I. Introduction

This is a portfolio report for Information Assurance & Security (CSE 543) course taken in Fall 2018 semester. For this course, we chose to do research on various smart home devices like IP cameras: Belkin Netcam and Drop cam, Amazon Echo, Google Home, Microsoft Cortana, Apple Siri which are voice assistant AI, smart light bulbs: Philips Hue, smart sprinklers, smart locks, smart TV, switches and Cisco Trustsec platform.

Nowadays, homes are evolving into smarter places by incorporating IoT (Internet of Things) devices. These devices helps in improving home physical security, energy efficiency, entertainment and comfort [1]. According to Oxford Dictionary, the term "smart home" is defined as "a home equipped with lighting, heating, and electronic devices that can be controlled remotely by smartphone or computer".

However, the increasing prevalence of smart-homes with Internet-connected devices creates security concerns at unprecedented levels. The large heterogeneity in IoT devices, each with its own hardware, firmware, and software, makes the security vulnerabilities diverse and the attack vectors manifold. Moreover, with the rise of cheaper IoT devices, vendors do not want to spend "unnecessary" time in testing the products thoroughly before they release the products to mass consumers. Thus, there are vulnerabilities that are waiting to be exploited in these devices. For consumers, these IoT devices are operated in a black box environment and the consumers have no ideas of the vulnerabilities lying in each of these IoT devices.

Through this project, the team wanted to inform users about the vulnerabilities that IoT devices have as well as propose possible solutions to harden the communication of these devices. Each member of the team, had independent tasks and responsibilities with regards to the devices and tools, to research,read papers and articles and find possible vulnerabilities and solutions.

II. Explanation of the solution

For this project, we divided the IoT devices, amongst our self, with each member working on atleast 2 types of smart devices.The leader and group leader took IP cameras: Belkin and Drop-cam. Others had devices like Cisco Trustsec Platform, mobile phone connected with home automation, smart sprinklers, smart locks, ZLL protocol for smart light bulbs, Intelligent Voice assistant,Smart TV, WeMo switch and lastly, strategic principles, and challenges in smart connected homes.

After selecting the devices, each member had to research and read published papers and journals on the topic, understand the working on the device, possible vulnerabilities in them, which part is most vulnerable and if possible a solution to prevent or remove those vulnerabilities.

There are various companies that manufacture and sell a specific IoT device, and every one of them have their own features, standards and principles that they follow. To keep things simple and easier, the team chose a specific company device which are both famous and for whom a lot of extensive research, papers, journals and analysis is done.

A. IP camera

IP cameras are devices that connect to servers located in the Internet.When used with out-of-the-box configurations, these devices are vulnerable to attackers located in the Internet because of their easily-guessed or none value passwords. Hence, this leads to a leakage of privacy and security of IP cameras' owners. In the Belkin Netcam, a lot of ports, remain open and any user within the local network can telnet into the device with default credentials admin:admin and is granted root access. It was also found that when the device communicates with the server, it does so in plaintext with information like MAC address of the device, username, video flicker rate, quality of video, etc. being part of the packet.

B. Smart Lock

There are several security variations to the simple lock and key system that has been incorporated in the IoT devices like use of passwords, a secret code, smart card, tag and smartphones, using wireless technologies like ZigBee, Wifi and Bluetooth for unlocking and locking the door. The August Smart Lock uses Bluetooth and Wifi for securing the home, it classifies the users into either OWNER or GUEST.

August Smart Lock is considered one of the best in the category of Smart Locks. Some of the best features that the locks has includes: date-time sync in the server, so that users cant fool the system by changing the time of the device. Encrypted TCP packets, which prevents hackers from knowing the contents of the packets and each packet has a unique token, which cant be used for replay attacks.

There are still some vulnerabilities that the smart locks have like

- Password attack, where any malicious user can change the password, create itself as the Owner and remove the original one.
- If the Auto-unlock feature is enabled, then if the malicious user gets hold of the owner phone, they can unlock the doors, without entering any sort of password, key or code. They just need to be in the vicinity of the house to unlock the doors.
- The APK Extractor, can decompile the application code, reveal the source code of the App and thus help determined adversary to probably reverse engineer most of what the app does.

C. *Intelligent Voice Assistant, Smart TV*

Voice assistants perform a wide variety of functions like change music, order groceries, open applications and lots more, they have become a ubiquitous part of the human life. Each of them have main 2 parts/components. First is the client side component, which are the actual hardware like microphone and speakers. And the second part, is the cloud component which takes in the user voice commands, performs computations and returns the results. Using these connections, there are various attack vectors which can be exploited.

- Passive listeners: most of these assistant use a "wake-up" word to start recording and to give a response. Compromised devices, could leave the recording on all the time and send all the recordings to the attacker.
- Sensitive Data collection: Any attack on the data centers, which hold the voice commands and the information of the user, including sensitive info can be leaked if there is an attack on the voice assistants data center.

Smart TVs nowadays have internet connections, microphones, cameras, apps, amongst various other things. These features comes with a wide array of security concerns and vulnerabilities, with the biggest problem being that the manufacturer can take long amounts of time to fix security vulnerabilities and only support devices for a few years.

D. *Smart Light Bulbs & Switch*

The smart lighting system allows a user to wirelessly control bulbs in the home, adjust intensity, custom colors, etc. via Android and iOS apps remotely. The remote control is supported by the cloud server and communicates over the internet. Each user needs to pair with the bridge, where the user's identity is whitelisted.

The packets captured from the communication between the Bridge and the mobile app, are in plaintext, allowing an attacker present in the home network to read all the commands sent to the bridge, as well as get a whitelisted user identity, which is used to gain access and control the bulbs.

Belkin smart switch provides a platform for users to control their household electrical appliances remotely. Both the app and switch are connected to internet and communicate via the Belkin maintained cloud server, this communication is completely plaintext and could potentially allow malicious users to control appliances.

One of the solution to the above problem of malicious users remotely controlling the devices, is to use SaaS (Security as a Service), its an external entity used to maintain the database consisting of access control rules that secure various IoT devices in a smart home environment. The rule database maintained externally can be updated with new vulnerabilities as and when they emerge. All the sources and the destined smart home devices like, Hue bulbs or WeMo smart switches are listed in the SaaS rules and are allowed access via the legitimate IP source addresses listed as legitimate user phones. [13]

E. *Smart Sprinklers*

Existing sprinklers, face issues like water wastage since they do not have any mechanism to detect and communicate whether there are any leakages in the system or not. Plus, they cant be accessed remotely.Rachio Smart Sprinkler resolves these issues and makes it convenient to install and use the controller, since its compatible with the existing ones and uses a set number of parameters with forecasted weather conditions to water only if necessary, thus restricting water wastage and cutting water bill cost for owners.

III. Description of the result

A. *IP camera*

Belkin Netcam is vulnerable to access by default passwords and researchers have proposed a potential solution for protecting IoT devices by employing software defined networks (SDN), which separates the control plane and the data plane. Instead of the switches performing the computation to route packets, the SDN controller will decide whether a packet is allowed or denied and perform the routing computation and to implement network-level security across the entire range of devices instead of the device level security.

B. *Smart Locks*

In general. the August smart lock does not have any major vulnerabilities in them, many other manufacturers do face issues like communication between the server and client in plaintext, replay attacks where packets are captured and relayed back to the device, amongst others. Unlike a conventional deadbolt and key, which cannot compromise thousands of homes at once, a savvy attacker discovering a new vulnerability could theoretically sell the access to homes of smart lock users worldwide.

C. *Intelligent Voice Assistants and Smart TV*

With the widespread use of the voice assistants, and new features being added on each year, attack vectors keeps growing and have the potential to cause larger amounts of harm if security patches do not keep up with new exploits. Users need to be wary of what they say around the devices and companies need to research in ML algorithms, and add security before critical actions are taken by the device like ordering groceries, opening a web page,etc.

Smart TVs are increasing dangerous devices, in terms of network and computer security. Their attack vectors are very large, with little or no security protection against them. It important that the manufacturers restrict the type of file that can be used, develop a semi-closed devices, with anti-malware services, that would at least give users a better opportunity to make sure their devices and network have not been compromised.

D. Smart Light Bulbs & Switch

Smart home IoT devices like Philips Hue bulbs and WeMo switches communicate with the user mobile app using plain text. As various devices are manufactured by different manufacturers, it is difficult to provide unanimous device-level security enhancements. Hence, security improvements are needed on the network-level to avoid potential attacks.

E. Smart Sprinkler

Since the demand for water will keep rising as the population increases, it is important to not just use water for right purposes but also in an efficient manner. Using the smart sprinkler controller helps in reducing the amount of water that is used for outdoor purposes and saves on water bill cost as well as for its owners there is an added incentive that the smart controllers are mostly compatible with the existing systems, thus adding to the convenience and ease to install and use.

IV. Description of my contribution

A. Research, Paper Gathering

I was responsible for gathering the relevant research papers and journals for the project, since the project required reading and collecting information and resources from various sources, thus, had to go through over 50+ papers, articles and journals, gather relevant topics and devices, which could be used for the project, since there are multiple manufacturers that are there for a device.

B. Smart Locks and Sprinklers

I was responsible for researching about the Smart Locks and Smart Sprinkler Controllers, researched about the various smart locks which are available in the market, differences between them, working of the smart lock, security features and shortcomings in the same. Most of the smart locks use some or the other sort of wireless technology for communication like WiFi, Bluetooth, ZigBee or NFC. One of the most unique thing about the August Smart Lock, is its auto-unlock feature, which locks or unlock the door, automatically when the user/ OWNER is in proximity range of 50 metres. Besides that the device also uses encryption for communicating with the server, making it resistant against replay attacks, or it being responsible for leaking sensitive user information.

Since water is one of the most precious resources that humans have, its important to use it consciously and not waste it, smart sprinklers helps in doing that by using a set number of parameters, weather forecast and smart detection of the water flow to use water and active sprinklers only when necessary and reduce wastage, and water bill cost for its owners. Rachio is one of the best smart sprinkler controllers out in the market today, since it is compatible with most the existing controllers, making the replacement and management easier and efficiently detects any water leaks and flow of water.

C. Report Writing and Review

I was responsible for the reviewing the overall final report of the project, create the class presentation, containing answers to many of the questions asked regarding my research devices: Smart Locks and Sprinklers. I was also responsible for write up on the 2 devices as well as the introduction and conclusion.

V. New skills acquired

This project was specifically very enlightening and full of interesting topics, facts and methods.

1) IoT: Learnt a lot about the IoT, how they are shaping our lives, how we are dependent on them, their inner workings and functionalities.
2) Smart Homes: Different types of devices that makes a home smart, the interactions between various devices and their purpose or use in our lives.
3) Vulnerabilities: Learnt about the vulnerabilities, how a simple device like a switch or a lock could be used to cause devastating effects. Common flaws in the devices, how manufacturers in order to cut costs on research and development, many times skip or dont do proper testing and release a device full of bugs and flaws.
4) Implications of the vulnerabilities: Any IoT device vulnerability can have grave implications on the lives of the humans. If the voice assistant or the smart Tv is hacked, the hacker could listen to private conversations, misuse the information and record personal details and activities.
5) Importance of Testing and Bug Fixes: Its important to test the application and device as thoroughly as possible before releasing it for the public use and to fix the bugs as possible to they are discovered so as to minimize the cost or the effect.
6) Hacking Techniques: During the research on the IoT devices, I learnt about the techniques (conventional and non-conventional) ones which are used to hack a device, gain control and misuse the device for ones own advantage.

VI. Team Members

The group consisted of 9 members which included: Nahid Ul Islam, JaeHyo Jeong, Vu Coughlin, Sameer Kulkarni, Chirag Bhansali, Pranav Havanurkar, Reece Bailey, Saurabh Abhale and Akash Rathi

References

[1] Noah Apthorpe, Dillon Reisman, Srikanth Sundaresan, Arvind Narayanan, and Nick Feamster. Spying on the smart home: Privacy attacks and defenses on encrypted iot traffic.

[2] Peter Ha, Smart Locks, Secure or Just Dumb? [online], Available: https://gizmodo.com/are-smart-lockssecureor-just-dumb-511093690, 2013

[3] Hollister, S. August smart lock and connect review: I'll use keys, thanks. [online], Available: http://gizmodo.com/august-smartlock-and-connect-review-ill-usekeystha-1685319060, 2015.

[4] Muhammad Sabirin Hadis, Elyas Palantei, Amil Ahmad Ilham and Akbar Hendra "Design of Smart Lock System for Doors with Special Features using Bluetooth Technology", 2018 International Conference on Information and Communications Technology (ICOIACT)

[5] Siddhi Kavde, Riddhi Kavde, Sonali Bodare and Gauri Bhagat (2017) "Smart Digital Door Lock System Using Bluetooth Technology", International Conference On Information, Communication & Embedded System (ICICES 2017).

[6] How we use water, [online], Available: https://www.epa.gov/watersense/howwe-use-water.

[7] Megan Fuller, Madeline Jenkins, Katrine Tjølsen "Security Analysis of the August Smart Lock"

[8] Wollerton, Megan, "Have a Smart lock? Yeah it can probably be hacked ", [online], Available: https://www.cnet.com/news/have-asmart-lock-yeah-it-can-probably-behacked/ ,2016

[9] Ho, Grant, et al. "Smart locks: Lessons for securing commodity internet of things devices." Proceedings of the 11th ACM on Asia conference on computer and communications security. ACM, 2016

[10] Samantha Bartram, From Simple Sprinklers to Smart Irrigation, [online], Available: https://www.nrpa.org/parksrecreationmagazine/2015/may/from-simplesprinklers-to-smart-irrigation/ ,2015

[11] Rachio Smart WiFi Sprinkler Controller and Wireless Flow Meter, [online] Available: https://www.rachio.com/how-it-works/

[12] Rachio App [online], Available: https://www.rachio.com/app/

[13] Sukhvir Notra, Muhammad Siddiqi, Hassan Habibi Gharakheili, Vijay Sivaraman, Roksana Boreli "An experimental study of security and privacy risks with emerging household appliances", 2014 IEEE Conference on Communications and Network Security