Designing an Effective IoT Security Course

A Technical Report
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Eric Sakmyster

with

Ryan Lenfant

April 24, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Eric Sakmyster

Technical advisor: Felix Lin, Department of Computer Science

Designing An Effective IoT Security Course

Ryan Lenfant*
rpl8af@virginia.edu
University of Virginia

Eric Sakmyster
ems5fa@virginia.edu
University of Virginia

ABSTRACT

Given their popularity, Internet of Things (IoT) devices and their safety have been at the forefront of technology research. As new devices are more popular and vulnerable, it is imperative to educate developers of IoT devices that security should be a priority in the development and production stage. Studies have shown that consumers expect manufacturers to put in proper protections to ensure their devices are safe, but newer devices continue to be more susceptible to exploits. Keeping the current mindset of producing devices without focusing on the security of the user will make homes more vulnerable to hackers over time. To address privacy concerns associated with IoT, universities can develop an IoT security course. Developing this course would entail discussing topics related to the various hardware aspects of IoT devices and how to exploit vulnerabilities within these systems. Additionally, there would be a lab section covering different devices and pieces of hardware such that a student could replicate previous exploits on old IoT devices. Through this course, future employees of IoT companies will adopt a security mindset in their development and the overall security of home IoT systems will be improved.

1 INTRODUCTION

The security of technology has always been a large issue that affects many people. In 2010, it was found that 560 million people were impacted by Internet crime loss [2]. In 2014, federal agencies reported 69,851 cybersecurity issues, a number which increased by 10% to 77,183 in 2015. As technology grows, so do security threats. This is an issue because there are not enough security professionals to combat the growing security concerns [4]. One of the largest technology fields lacking security experts is IoT (Internet of Things),

IoT refers to the networked interconnection of everyday technology which communicates to humans and other devices [13]. It aims to improve the quality of life by making useful data comprehensible to humans and by handling data transfer on the back end of devices. It is becoming a common necessity that all people should own and will be essential in the future [1]. IoT devices are so convenient that they are extremely popular with many people and are mass-produced. "There were an estimated 12.5 billion IoT devices, almost twice as much as the world's population of 6.8 billion" [11]. Due to the sheer variety and vast amount of IoT devices, it is imperative to invest in more security, so a user's valuable information is not stolen. This is further emphasized by the fact consumers do not understand the security risks of owning IoT devices and expect manufacturers to put the proper protections in place to ensure their devices are safe [14]. Security should be made a priority when developing any technological device. If we keep the current mindset of producing devices without focusing on the security of the user, homes will become more vulnerable to hackers as time goes on. Studies show technology coming out is extremely susceptible to exploits as the technology is so new, drawing importance to focus on safety in the development stage [7]. To improve the climate of trying to focus on profits to the ethically safe IoT devices, a system of "cyber hygiene" must be taught to those that develop and use these devices [8]. This would include educating a user on the security features of the devices they use, constantly updating devices to have the most secure software, and forcing the user to change their password regularly.

Although educating users and developers would benefit the security of society, many colleges and businesses do not require a security course. Undergraduate degree programs focusing on information security are needed [12]. The lack of an undergraduate security curriculum is due to the lack of an "academic and practitioner consensus on which courses matter and which do not" [3]. It is hard to determine what skills are useful for students to know to ensure safe IoT devices are created. This is not to say there are not general topics that will greatly benefit students in the security sector. One such topic which benefits all students, especially those going into the security industry, is a security mindset. It provides valuable skills all students can benefit from regardless of their career interest[9]. These include vital skills such as the ability to identify and fix bugs, write efficient code, and test programs for deficiencies. Including security courses in a computer science curriculum will teach students important skills which will help them throughout their career and improve the security of IoT devices produced in the industry. Industries rely on colleges and universities to produce qualified employees who can handle security problems [10]. Through the utilization of an IoT course in higher education systems, developers will prioritize the safety of a user and address security concerns as they appear.

*Both authors contributed equally to this research.

2 RELATED WORK

Many colleges offer graduate-level classes for IoT security. For example, Virginia Tech offers a "Cybersecurity and the Internet of Things" graduate-level course that teaches students "the engineering architecture components (hardware, protocols, and technologies) of the evolving IoT ecosystem, motivated by the core principles of cybersecurity"[5]. The University of Virginia also provides a "Mobile and IoT Security" graduate class that "focuses on aspects of system security that arise in this challenging and ever-evolving space of mobile communication systems, primarily focusing on smartphones and IoT platforms"[6]. While both these courses offer similar topics to the IoT Security course, neither provides a chance for students to build a minimal IoT device to gain hands-on experience. This is something that will help them in their transition to the industry. Additionally, providing an IoT security class to undergraduates is beneficial for those going straight into industry and not graduate school so they have the chance to take such a class. Otherwise, students may join an IoT company lacking security education, and the company may not stress security. This contributes more to the problem of IoT devices not being secure.

The courses Introduction to Cybersecurity (CS 3710) and Computer Architecture (CS 3330) at the University of Virginia teach concepts that will be taught in the IoT Security course. Introduction to Cybersecurity is a broad overview of security concepts and exploits that can be applied to many applications of computer science. Because of this broadness, there is not as much applicability to real-world devices and how these exploits might differ between them. With hands on projects, students are forced to implement security principles in practical ways, with the hope that this will achieve a security mindset more effectively than an introductory cybersecurity class. Computer Architecture is an integral course in understanding hardware used inside of IoT devices, specifically computers. From this course, students should know how a generic processor would work for an IoT device, as well as see assembly level programming of hardware that could be exploited. To further the understanding of these ideas, it would be beneficial for students to see how these hardware components work in physical devices, not just simulations. Additionally, attacks on IoT hardware can be seen in person by students so that they can better understand how to make that hardware secure. Overall, an IoT security course could build off both these existing University of Virginia courses, adding needed specificity to the concepts taught in them.

3 SYSTEM DESIGN

The IoT Security Course is a proposal of a new course for any college to implement. Some concepts are borrowed from the UVA courses Computer Architecture and Introduction to Cybersecurity, but more focus is placed on IoT devices. This course is designed to teach students about the security issues surrounding everyday IoT devices such as smartphones, cameras, and healthcare equipment. Students will learn how to find, analyze, and protect against various exploits in vulnerable IoT devices.

3.1 Syllabus

A syllabus governs the structure of the course's policies, lectures, assignments, exams, and topics covered. A professor teaching the course or a student taking it can refer to the syllabus at any point in the semester for clarification on aspects of the class.

Prerequisite classes and skills are defined by the syllabus in order for a student to succeed. Students are required to have taken Program and Data Representation (CS 2150) and Computer Architecture, or an equivalent of each, before taking the course. Program and Data Representation is important for a student to know the various data structures used in the creation of IoT devices, particularly for data collection and security protection. It is also expected that students come into the course knowing a form of low-level programming language, with a strong emphasis on C, which Program and Data Representation covers. Most programming components of lab assignments in the class would use C so that students can be programming closer to the actual hardware of an IoT device. Computer Architecture gives students a solid foundation with the hardware components of a computer, allowing them to better understand topics about IoT hardware. Students also would have gotten experience with x86-64 assembly in Computer Architecture, which will be helpful for programming hardware for IoT, as well as understanding exploits of IoT. While this class goes over security topics talked about in Introduction to Cybersecurity, a student does not need to have taken that course to take the IoT Security course.

Key objectives the course hopes to emphasize for students are outlined in the syllabus. Students will gain experience with various IoT devices and the hardware in them. Through this objective, students should understand how common IoT devices interact with each other through hardware components, as well as the software that makes this possible. Students will learn about the modern exploits of IoT devices. With this knowledge, students would be able to recognize, or even prevent exploits of IoT devices they would make in industry. The course will prioritize creating a mindset that security should be a priority in the development and production stage of IoT software. Along these lines, students will learn better security-oriented programming skills through the topics taught and programming assignments.

A detailed weekly schedule of topics taught and a brief description of what the week of lectures and assignments will cover are presented at the end of the syllabus. At the beginning of the course, students will be taught an overview of what IoT entails, including defining features in most IoT devices. Students will then learn about current ethics and security standards related to IoT. Ethics behind hacking will be discussed so students do not replicate exploits they learn in the class in a malicious way, but instead use exploits as a way to further security in the IoT industry. To build on Computer Architecture, students will then learn about IoT hardware and be able to see these physical components themselves in lecture. Once this knowledge has been established, physical attacks will be covered, including physical tampering of IoT devices and exploits that can be achieved through UART. This will allow students to diagnose more externally related security problems with IoT devices. Following these topics, a shift will be made towards learning about an IoT network. Students will be taught about network components, such as routers and nodes, and how IoT devices communicate with each other using the TCP/IP model. Network attacks on IoT devices will then be presented, which will include denial of service, man-in-the-middle, and botnets. Students will experiment with different defenses of these attacks to learn how to prevent them. After the topics on networks, students will be taught about security-oriented programming in a broad context to emphasize the importance of it for all programming projects, but also in the scope of IoT. Current security practices in programming for the IoT industry will be analyzed, including the downsides of agile development and improvements that can be made to it to promote greater security. All these topics lead up to four weeks at the end of the semester where students will implement a trivial IoT device using a Raspberry Pi 3. This will allow students to apply what they have learned about IoT hardware, as well as how to implement security principles they have learned about in the course. To close the course, IoT creators from the industry will present to students to talk about their experiences.

3.2 Lectures

Lectures for this course would follow a Monday, Wednesday, Friday 50-minute schedule. The setup of a typical lecture would involve a slideshow of the day's material, and interactive elements where students can use IoT devices or examine hardware in them. Each week of lecture will correspond to a weekly topic that is presented in the syllabus course schedule. Most weeks will include a case study lecture for the material covered in that week. This case study will apply the concepts to the real world, such as seeing how certain exploits have affected household IoT systems or how smart cities set up such a large IoT network effectively. This will connect the material learned in the lecture with real world examples so students can better understand the material.

3.3 Lab Assignments

Every week students for homework will have to complete a lab assignment. Lab assignments will be assigned after Friday's lecture each week, and will cover what was discussed that week. Student's will then have a week to complete the assignment. These assignments will be individual, but will mostly be experimental in nature, in that failures in the assignment can be explained by the student. The labs will cover different IoT devices and pieces of hardware such that a student could replicate exploits on old IoT devices or examine IoT device behavior. The format of the assignment will consist of either a programming component, a typed report, or both. When exploits are taught in the class, lab assignments will include students attempting them, reporting observations, and writing a report on possible defenses that they research. If the exploit must be coded, students will have to program that with some guidance from the lab instructions. Other labs will consist of understanding fundamental behaviors of IoT devices, which will include writing a report reasoning about the behaviors. Most labs will deal with a physical IoT device that students will be provided with, which could be trivial IoT devices like a Ring doorbell or a computer camera. However, some labs will not be possible for students to use actual IoT devices, so these labs will entail using a simulation or virtual machine. Wireshark will be a key component of most labs to examine network activity happening with an IoT device. Students will be introduced to Wireshark and how to use it in the introductory lab assignments.

3.4 Creating an IoT Device

At the end of the course, students should have the necessary skills, with assistance, to create a trivial IoT device and implement security measures they have learned about in the course. To do this, a Raspberry Pi 3 (RP3) will be used as the computer system behind each student's IoT device they will make. RP3 basics will be taught to students and lots of guidance will be given for more complex implementations. This end of semester project will be as open-ended to students as possible, and they will be asked to implement certain features of their choosing. Through physical interaction and programming of actual hardware, students will get to experience what it's like to make IoT devices in industry. The major portion of this project will be a TA or the instructor presenting an exploit or vulnerability to the student for their specific IoT device. The week after the exploit is given to the student, the student will be expected to try and implement defenses against it. While students' IoT implementations and

security vulnerabilities may vary, common defenses to implement are likely between projects. Common defenses that most students will need in their projects will be presented in lecture the week of this portion of the project to assist students. The project's grading will come from lab assignments associated with each week of the project.

4 PROCEDURE

4.1 Use By Instructors

The course syllabus can be a useful tool for professors to create an effective IoT security course. As emphasized by the syllabus, the course should try to make the classwork mirror identical scenarios to that of the industry. To do this, instructors should aim to have one case study a week, as well as a lab that allows students to work with material relating to the case study. This will allow students to connect with the case study to better understand why the security breach happened and how it can be prevented in the future. The lecture should be utilized to teach students the skills they need to complete the labs and any information they may need to understand the case study. By focusing on a core topic each week and reiterating the lecture material through the case study, students will have a whole week to digest and understand the material.

With the course lectures and labs also comes creating an IoT device at the end of the semester. Instructors should aim to give students some free reign on this assignment and allow students to try and implement vulnerabilities and defenses they learned throughout the semester. This will teach them how to create an IoT device on their own while also considering the security during the development phase of the device. Each week instructors should ensure that students are making progress on the device by checking for a feature, vulnerability, and defense mechanism. In the end, students should develop a functional device that can defend against other exploits from other students.

4.2 Use By Students

Students can get the most out of this course by exploring the material and case studies examined through the course. They are encouraged to find their own examples of exploits happening in the world around them to get a grasp as to how vulnerable the world of IoT is. In doing the labs, students will learn how to implement different attacks and defenses of IoT devices. This will help them learn how to identify and stop various types of attacks they may face in the industry. In developing their IoT device, students will use their knowledge of the structure of an IoT device, as well as attacks and defenses, to create a secure and safe IoT device that fulfills a purpose. Students will gain a security mindset by focusing on the security of their IoT device and learn vital skills to becoming a security professional.

5 RESULTS

Through the development of a syllabus, lectures, and lab assignments, an effective IoT security course can be developed. The course was designed to keep security at the forefront of all IoT development. The material produced to create the course such as the syllabus, lectures, and assignments were shared with students who have taken Computer Architecture or Introduction to Cybersecurity to assess the feasibility and popularity of the course. In sharing this study with these students, they were excited about the prospect of a niche undergraduate security course. As the University of Virginia does not have a pure Cybersecurity major, they thought it was a good inclusion for students who want to join the cybersecurity industry. The students interviewed also concluded that it would promote more students to take security courses given the popularity of IoT. They thought that the lab and case study structure would give students a better idea of how privacy issues are tested for and analyzed in the industry.

In regards to the material associated with the course, students felt the course covers a diverse set of topics within IoT. They appreciated that the course did not stray to topics outside of IoT and the inclusion of both physical and virtual attacks. The section of the course students were most interested in was the Raspberry Pi project where the students create their own IoT device. It provides them with industry experience in creating an IoT device, testing the device for vulnerabilities, and fixing vulnerabilities when they occur.

6 CONCLUSION

By creating this course, we acknowledge that there is no universal remedy to combat all security issues in the IoT industry. Technology is rapidly advancing and it can be hard for security to keep up with it's evolution. One way to mitigate these issues is through security courses at higher education systems. This undergraduate IoT course was designed to meet the rising need for security experts in industry. The lack of security professionals in industry is a growing problem that needs to be addressed [4]. As there are a lack of undergraduate programs focusing on information security [12], it is imperative to develop and provide undergraduate courses such as the one presented in this paper. Courses such as this will produce employees with valuable security skills which they can incorporate into their practices while in industry. Through lab assignments and case studies, undergraduate students can directly translate material they have learned from the course to the workplace. The course aims to prepare undergraduate students for work as they may not

attend graduate school and have the opportunity to take a course like this.

Teaching IoT can be difficult as the content ranges across a variety of topics. These topics can vary from different types of attacks to the physical components of a device and how it functions. One student pointed out in viewing the material that they were glad the course strictly focused on IoT related topics instead of general security topics. The course should build off introductory level security courses such as Introduction to Cybersecurity, however, content must remain distinct between the two courses to have the most impact on students. A feature of the course that makes it distinct from other security courses is the creation of the IoT device at the end of the semester. Given the interest expressed by the student to do this section of the course, the creation of the undergraduate course should be considered. The project at the end of the semester allows students to implement and test their security mindset. This valuable skill will help them with their future career [9] and produce more developers who can be integrated directly into industry. The project at the end of the semester, course topics, and lab structure are key to making the security challenges faced in class as realistic as possible, addressing the issue of a lack of a curriculum[3]. By producing a course that mirrors security issues faced by everyday industry, students will be better prepared for the workplace and improve the security of society as a whole.

7 FUTURE WORK

Creating a full course can often take years worth of planning. Given the time constraints of the capstone project, it can be hard to produce a full course with lectures and assignments for each week. With more time to work on the course, we would first work out the details of the Raspberry Pi project and create an example which students could observe to get a better idea of what to do for the assignment. This assignment is a core part to teaching students how to focus on security during the development stage of an IoT device. It would also be beneficial to come up with workshop sessions where during this project, students could work in a certain classroom with other students and teaching assistants to get feedback on the progress of their project. This would imitate industry so that students are not just working individually, but they also get to be creative in having their own projects. The second section we would work on are the lab assignments. With more time, we would work to create labs for each of the subjects. This would include various learning objectives as well as finding various IoT devices with vulnerabilities for students to exploit. A key component missing from the current description of the labs is adapters that would have to be used to allow for both communication with certain IoT devices and exploits that would otherwise be difficult for students to do. The final section we would want to build upon are the lectures. This would involve making lectures and finding case studies for each topic in the course. It is also important that lectures are interactive, so thinking of certain IoT devices that can demonstrate the week's material that can be brought into class would help engage students better. Once each section has been addressed, the goal would be to implement this course as an elective to see if it is effective at teaching students IoT security.

REFERENCES

[1] Aman Arora, Anureet Kaur, Bharat Bhushan, and Himanshu Saini. 2019. Security concerns and future trends of Internet of Things. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, Vol. 1. IEEE, 891–896.

[2] Michael Lesk. 2011. Cybersecurity and economics. *IEEE Security & Privacy* 9, 6 (2011), 76–79.

[3] Robert McCreight. 2009. Educational challenges in homeland security and emergency management. *Journal of Homeland Security and Emergency Management* 6, 1 (2009).

[4] Andrew McGettrick et al. 2013. Toward curricular guidelines for cybersecurity: Report of a workshop on cybersecurity education and training. *Association of Computing Machinery (ACM). Retrieved from https://www. acm. org/education/TowardCurricularGuidelinesCy bersec. pdf* (2013).

[5] Virginia Tech Bradley Department of Electrical and Computer Engineering Graduate Programs. 2021. ECE 5480 - Cybersecurity and the Internet of Things. *Retrieved from https://ece.vt.edu/grad/courses/5480* (2021).

[6] University of Virginia Department of Computer Science Graduate Programs. 2021. CS 6333 - Mobile and IoT Security. *Retrieved from https://sites.google.com/virginia.edu/mis19/home* (2021).

[7] Dennis Kengo Oka, Takahiro Furue, Lennart Langenhop, and Tomohiro Nishimura. 2014. Survey of vehicle IoT bluetooth devices. In *2014 IEEE 7th international conference on service-oriented computing and applications*. IEEE, 260–264.

[8] Jo Ann Oravec. 2017. Emerging "cyber hygiene" practices for the Internet of Things (IoT): professional issues in consulting clients and educating users on IoT privacy and security. In *2017 IEEE International Professional Communication Conference (ProComm)*. IEEE, 1–5.

[9] Vahab Pournaghshband. 2013. Teaching the security mindset to CS1 students. In *Proceeding of the 44th ACM technical symposium on Computer science education*. 347–352.

[10] Jeff Sauls and Naveen Gudigantala. 2013. Preparing information systems (IS) graduates to meet the challenges of global IT security: Some suggestions. *Journal of Information Systems Education* 24, 1 (2013), 71–74.

[11] Vijay Sivaraman, Hassan Habibi Gharakheili, Clinton Fernandes, Narelle Clark, and Tanya Karliychuk. 2018. Smart IoT devices in the home: Security and privacy implications. *IEEE Technology and Society Magazine* 37, 2 (2018), 71–79.

[12] Belle Woodward, Thomas Imboden, and Nancy L Martin. 2013. An undergraduate information security program: More than a curriculum. *Journal of Information Systems Education* 24, 1 (2013), 63.

[13] Feng Xia, Laurence T Yang, Lizhe Wang, and Alexey Vinel. 2012. Internet of things. *International journal of communication systems* 25, 9 (2012), 1101.

[14] Serena Zheng, Noah Apthorpe, Marshini Chetty, and Nick Feamster. 2018. User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–20.