Ali Mirabzadeh

305179067

CS 111: OS Research Report, IoT

IoT, Security and Privacy

From simple tasks such as motion-activated light switches to complex tasks such as controlling the traffic lights in smart cities Internet of Things, IoT, has been becoming an inevitable innovation of the 21st century due to their large market and potential in different industries. IoT is a system that integrates physical processes with digital connectivity. Therefore, such an applicable technology would not come out without its issues and challenges. Even though IoT has applications in different industries and sectors, the main emphasize and focus of the research article is on consumer IoT due to its largest number of applications and since it’s the most significant market. For our purpose, aerospace industry, the study of IoTs’ security and privacy issues would help us to improve our own implementation of IoT. The article, first, studies five major IoT programming platforms to help us to understand their program structures. Second, studies IoT specific issues, IoT program idiosyncrasies and general precision requirements for IoT app analysis. And, lastly, studies six IoT analysis systems from literature for security and privacy that incorporate program-analysis techniques. In other words, it talks about main three domains: IoT programming platforms, program analysis, and security and privacy.

As mentioned earlier, regardless of their application and their complexities, IoT devices often share the same structure; from bottom to top their architecture consist of devices, connectivity protocols, and IoT programming programs. “They use a cloud back-end to synchronize device states and provide interfaces for remote control and monitoring devices” (ACM Comput Surv, 3). Simply, IoT devices are equipped with embedded sensors and actuators that interact with a physical environment. Then the physical states and events would be sent to the hub/cloud and the magic happens. Now that we have a better understanding of IoT devices we can study the major IoT platform and how can we can approach about security and privacy issues. The five major platforms that are discussed in the article are Samsung’s SmartThings, OpenHAB, Apple’s HomeKit, Android Things, and Amazon IoT. The research article goes into details about all those aforementioned platforms, but it points out their common design feature. Based on the article, “IoT systems structure their apps’ design around the sensor-computation actuator idiom regardless of their purpose and complexity”. (ACM Comput Surv, 7)

Program-analysis goals such as Sensitive Data Leaks, Abuse Prevention, Permission Misuse, Data Provenance are a few a common goal in which some still remain open problems. Program-analysis techniques operate on IoT source code to achieve a variety of goals like understanding of apps’ security. They have been applied either statically, analyzing code of an app without running it, or dynamically, analyzing the code in run, possibly, under-instrumented condition to see if there are likely problems.

The article also mentions IoT-specific analysis issues in which have unique characteristics and challenges in terms of program analysis when compared to other platform apps. Physical Channels, Simulation and Modeling of IoT Programs, Automated Test-case Generation, Multi-app Analysis, and Interaction between IoT Devices and Trigger-action Platform Services are the five challenges that are mentioned in the article; with the main focus of security and privacy issues. The article also talks about IoT Application Idiosyncrasies such as RESTful APIs and Language-Inherited Operations to show that “each IoT has its own Idiosyncrasies based on how the structure the apps and the programming languages they use”. (ACM Comput Surv, 15). Towards the end of the article, the article offers fundamental analysis techniques. Taint Tracking, Code Instrumentation, Symbolic Execution, Model Checking, Program Slicing, and Opacified Computing are the ones that are mentioned in the article. For instance, Code Instrumentation “adds specific code to the source code of an app to collect the app’s run-time behavior” (ACM Comput Surv, 20). Even though the article doesn’t do a great job in going into details for each but gives us general idea of approaching privacy issues and analyzing them.

The main purpose of this article is educating on IoT and its security and privacy issues as those are new. The weakness of the article is not going into details for each topic; however, it does a great job on giving the readers background on IoT, different techniques and ways to approach the privacy issues. Therefore, for the purpose of our organization it’s a great article to gain some insight about IoT and its security issues and how to approach them through program-analysis techniques. The article gives us insight about different IoT platforms through surveying them; hence, we are able to distil the key aspects of program analysis under IoT-specific analysis issue, IoT app idiosyncrasies, and analysis sensitives. Through surveying different techniques and approaches, we can conclude that sensor-computation-actuator is the main structure within IoT devices, the security and privacy issues are subtle to find due to controlling IoT applications through devices, and a suit of analysis tools and algorithms targeted at diverse IoT platforms is at this time largely absent. There is still more work that needs to be done to improve the IoT security.

Work Cited

Celik ZB, Fernandes E, Pauley E, Tan G, McDaniel P. [Program analysis of commodity IoT applications for security and privacy: challenges and opportunities](https://arxiv.org/pdf/1809.06962.pdf). *ACM Comput Surv.* 2019;52(4):74. doi:[10.1145/3333501](https://doi.org/10.1145/3333501)