Seminar Talk: “IoT Security” (Speaker: Dr. Elisa Bertino)

Matthew Whitesides

Abstract

In today’s presentation, Dr. Elisa Bertino discusses the current challenges in securing the Internet of Things (IoT) related devices and systems. IoT applications span across all practical aspects of modern society, from commercial devices to consumer technology. All these devices gather and transmit sensitive data, and there exist various stages of attack vectors any bad actor may take. These expanded risks force security researchers to deploy many levels of protection for all IoT systems.

I. Introduction

INTERNET of Things (IoT) refers to the network of physical objects containing sensors, computing capabilities, and some form of networking with other devices. IoT devices use these features to send data to centralized servers or centralized other connected devices using various communication technologies. IoT using sensors and computational power enables a direct connection between the physical world and the digital, allowing us to automate systems, uncover hidden meaning in data, improve healthcare management, and infinitely more possibilities. Potential and current applications range from monitoring crops to factory and supply chain management to remotely monitoring patients and medical devices, such as implanted devices and infusion pumps. Suffice it to say, the area of IoT is an ever-growing multi-trillion dollar industry and impacts us daily, but this leads to a broad and attractive attack target for any bad actors in the system.

II. Background

While IoT devices bring a lot of exciting new possibilities, it also creates significant security concerns. Suppose medical devices, smart cities, agriculture, etc., will utilize IoT devices that collect and transmit sensitive data. In that case, some of the most critical aspects of our society will be open to cyber attacks. IoT device information often includes meta-data such as location, time, and context. This information is typically collected at the edge node IoT devices and uploaded or transmitted to cloud servers or processing nodes in a network. Given the energy and computational constraints these small IoT devices typically have, securing the data they collect is not an easy task. For example, a health monitoring device must collect sensitive medical data from a user, securely transmit it to another device (i.e., a smartphone), use low energy, with secure authentication, all while not forcing the user wearing the device to monitor its integrity constantly.

III. Research Contributions and Results

IV. Lessons Learned

V. Conclusion

Acknowledgment

The author would like to thank Professor Sajal Das with the Department of Computer Science, Missouri University of Science and Technology and Dr. Elisa Bertino with Purdue University.

References

[1] E. Bertino, “Data Security and Privacy in the IoT.”, 2018.

Matthew Whitesides Master’s Student at Missouri University of Science and Technology.