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

A. Encryption Protocols

In "A secure communication protocol for drones and smart objects." [2] Bertino et al. propose a secure and efficient communication protocol for drones and other smart devices. On top of being energy and computationally efficient, the authors novel protocol incorporates drone-specific required security functions, such as authenticated key agreement, non-repudiation, and user revocation. Drones are essentially mobile wireless sensor networks (WSN). However, mobile sensors introduce new security risks because mobile sensors are privileged nodes that store and transmit collected data exposed to physical capture by bad actors in the sensor network area. New encryption protocols must consider IoT device's wide-scale deployment and limited computational resources. In the end, the authors propose an efficient certificateless signcryption tag key encapsulation mechanism (eCLSC-TKEM) that reduces the time required to establish a shared key between a drone and a smart object over the existing protocols by using dual channel communication.

B. White-Box Encryption

In "A Secure Shuffling Mechanism for White-Box Attack-Resistant Unmanned Vehicles" [3] Bertino et al. discuss the challenges of designing a method of protecting unmanned ariel vehicles (UAV) from strong white-box encryption attacks. UAVs are essentially more complex IoT mobile sensors. They are mobile, collect and transmit data, and more often, this data is highly sensitive, making them attractive targets for malicious attacks. The concept of white-box cryptography was created to protect software implementations of cryptographic algorithms in untrusted environments that are not equipped with hardware-assisted security mechanisms. White-box attackers access and manipulate the internal memory by obtaining a root privilege and installing malware. White-box is the worst-case form of attack and requires complex solutions to protect against an attack that already has this level of privilege. To tackle this issue, Bertino et al. propose a lookup table shuffling mechanism in the context of unmanned vehicle applications and analyze the level of security this provides against attack. They prove that their shuffling protocol makes it difficult for a white-box attacker to successfully encrypt/decrypt any plaintext/ciphertext even if the attacker knows the entire lookup table.

C. Incident Response and Prevention

The theme of IoT security seems to revolve around the idea of resource constraints, unsecured operating environments, and less secure communication protocols, making them especially susceptible to operational failures and security attacks. Wireless sensor networks again are not an exception. Dr. Bertino discusses this generalized problem in the incident response and prevention section. In "a security incident response and prevention system for wireless sensor network." [4] Bertino et al. propose a security incident response system designed to keep WSNs functional despite data anomalies or attacks and recover from attacks without significant interruption called Kinesis. In highly critical implementations of IoT devices such as societal functions or military equipment, devices need to be operational and quickly recoverable from attack and interruption. This use case is particularly challenging in IoT devices due to their resource and communication constraints. Kinesis essentially is a program that monitors nodes and detects and responds to anomalies in the network. Kinesis selects the response based on the suspect's security status, and since it's distributed, it does not require any central authority to trigger the response actions. Kinesis enables quick and efficient response to incidents required by the constraints that IoT nodes are often under.

IV. Lessons Learned

In today's presentation, Dr. Bertino sheds light on the challenges involved in protecting IoT devices. It is impressive how fast the growth of IoT and related technologies are being incorporated into our modern world. However, these devices are the most susceptible to attack due to their limited computational capabilities, often deployed in unmonitored or unsecured environments. They contain some of the most sensitive information, such as medical devices or military equipment. These implications make you consider the impact of attacks on these devices. Dr. Bertino discusses various impressive methods of defending against attacks on these devices. IoT devices often support our most critical infrastructures, such as in modern smart cities. If a bad actor was successful essential functions of civil infrastructure could be interrupted, or sensitive data could be obtained. This use case makes IoT security not only the most challenging devices to secure but some of the most important. In particular, discussing the responder and prevention methods are often overlooked by research. What you do to solve the issue if security is breached quickly is just as important as protecting against it in many cases, especially in IoT environments where you may not have access to the devices themselves.

V. Conclusion

In the end, I would like to thank Dr. Bertino for introducing the various challenges and methods she has discovered for protecting IoT devices. IoT security is an essential and growing field of research that presents numerous challenges for the future. The research that Dr. Bertino and her team are doing is vital to securing the devices that are a big part of the future of modern society.

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.
[2] J. Won, S. Seo, and E. Bertino. A secure communication protocol for drones and smart objects. In Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '15, Singapore, April 14-17, 2015, pages 249–260, 2015.
[3] J. Won, S. Seo, and E. Bertino. A Secure Shuffling Mechanism for White-Box Attack-Resistant Unmanned Vehicles.
[4] S. Sultana, D. Midi, and E. Bertino. Kinesis: a security incident response and prevention system for wireless sensor networks. In Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems, SenSys '14, Memphis, Tennessee, USA, November 3-6, 2014, pages 148–162, 2014.

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