Towards Standardization of IoT Message Exchange Format for Intrusion Data Sharing

Gustavo Angeles, Advisor: Dr. Ambareen Siraj
Department of Computer Science, Tennessee Tech University

CERC Cybersecurity Education, Research and Outreach Center

ABSTRACT

The necessities of modern day lives today depend heavily on usage of the Internet of Things (IoT). Exponential growth of this technology has led to increase in security and privacy concerns. Heterogeneity of the IoT Sensors is a major limitation for security decision makers who have to extract and integrate data from different IoT sensors to assess overall security posture of the network. Current security solutions cater to homogeneous networks where devices use similar configurations and protocols for communication. In this work we describe the IoT Message Abstraction Format (IoTMAF), which is a first step towards IoT data standardization. IoTMAF is capable of abstracting wireless IoT protocol data without losing any of its significance. We demonstrate that IoTMAF aids in the detection of a complex attack targeting a fully heterogeneous environment.

In addition, we describe the eXploitable IoT ecosystem (xIoTec), which is intended to be used for heterogeneous IoT security research. xIoTec is a fully heterogeneous IoT security testbed. The testbed includes both network and physical attack vectors. Moreover, it implements the full IoT ecosystem taking account of user interaction with IoT devices and cloud services. We were able to conduct a security research experiment using this testbed by performing network and physical attacks using the IoT devices.

INTRODUCTION

- IoT provides a way for a physical systems to be connected to cyberspace [1].
- IoT is a heterogeneous environment by having its devices use different protocols for communication due to their need of power consumption, message length, communication distance and other factors.

PROBLEM DEFINITION

- Many security vulnerabilities with widely used IoT protocols such as ZigBee, BLE and Wi-Fi have been reported[2].
- No general standard is found making IoT data increasing the difficulty to analyze data for security purposes.
- There is a lack of fully heterogeneous IoT testbeds available, increasing the difficulty of testing heterogeneous IoT security solutions.

OBJECTIVES

- The aim of this work is to take a first step towards IoT standardization by developing an abstraction format which retains all protocol information and sensor data.
- This work aims to tackle the lack of testings environments problem by developing a fully heterogeneous IoT security testbed capable of collecting data at any point in communication.

METHODOLOGY

- Novel message abstraction format named IoTMAF
  - Abstracts heterogeneous IoT protocol data and sensor data into a common format.
  - Provides a better picture of a network's security health.
  - Implemented using JSON.

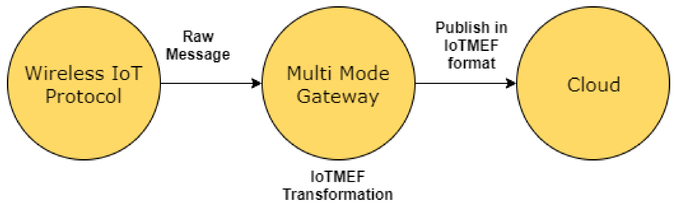

Figure 1: IoTMAF workflow

- Novel heterogeneous IoT security testbed xIoTec
  - Mimics a Smart Home/Building room with configurable IoT devices.
  - Incorporates several known IoT wireless protocols including ZigBee, Wi-Fi and Bluetooth Low Energy
  - Capable of collecting data from physical and network attacks at any point in communication.

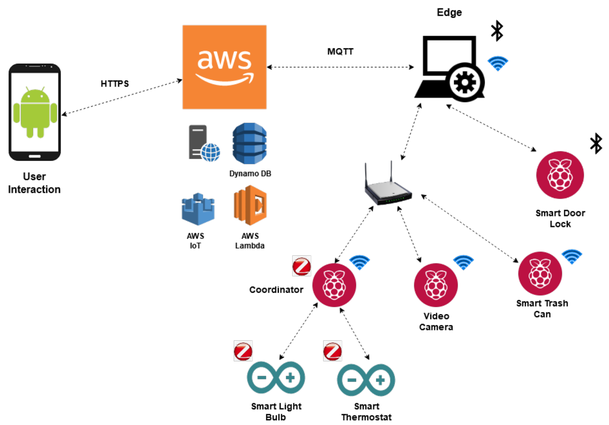

Figure 2: xIoTec Architecture

ATTACK SCENARIO

- Multi-protocol attack [3] targeting all devices in xIoTec.
- Includes physical and network intrusions.
- Attacker successfully retrieves sensitive information from a physical medium.

ATTACK DEPLOYMENT

- The attacker makes the following steps:
  - Video camera live feed replacement. (Network Attack)
  - Unlocks door lock. (Network Attack)
  - Walks into room. (Physical Attack)
  - Turns on lights. (Network Attack)
  - Retrieves sensitive information (Physical Attack)
  - Exits the room.

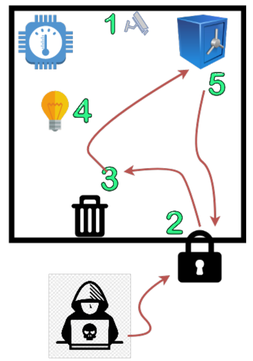

Figure 3: Attack Deployment

RESULTS

- Successfully detected the whole picture of the orchestrated attack.
- Detection of both physical and network attacks.
- Successfully integrated and correlated data using IoTMAF.
- Proven IoTMAF flexibility by adapting three completely unrelated IoT wireless protocols

CONCLUSION & FUTURE WORK

- The abstraction format provides a bigger picture of an attack
- First step towards IoT standardization with rooms for improvement
- Successfully collected intrusion and non intrusion data with the novel testbed.
- Future work:
  - IoTMAF implementation efficiency improvement.
  - Implementation in more resource constrained environment.
  - Addition of more protocols and devices to xIoTec.

ACKNOWLEDGEMENTS

- We would like to thank the Cybersecurity Education, Research and Outreach Center for providing the resources necessary to support this project.

REFERENCES

[1] GILCHRIST, A. 2016. Industry 4.0: The Industrial Internet of Things. Apress.
[2] Fadele, A., Othman, M., Hashema, I., & Alotaibi, F. (2017). Internet of things security: A survey. Journal of Network and Computer Applications, 88.
[3] Cremers, C. 2006. Feasibility of multi-protocol attacks. In First International Conference on Availability, Reliability and Security (ARES'06) (pp. 8–pp).: IEEE.