CERIAS

The Center for Education and Research in Information Assurance and Security

Internet of Things Mobility Forensics

Niveah Abraham, A. A. Bolaji, Hanlin Chen, Dr. Melissa Dark, Al Holt, Dr. John Springer

RESEARCH QUESTION:

What information can be derived from the OSI model for a Smart Home doorbell to conduct Confidentiality, Integrity and Availability test?

MOTIVATION

The purpose of this research is to use a smart doorbell as a target of investigation in the determination of information that can be derived from the OSI model for a Smart Home doorbell to conduct Confidentiality, Integrity and Availability tests. This project provides further information on available risks in the IoT ecosystem with the broader aim of identifying loopholes in IoT devices that are being deployed in the Smart Home environment for security related purposes.

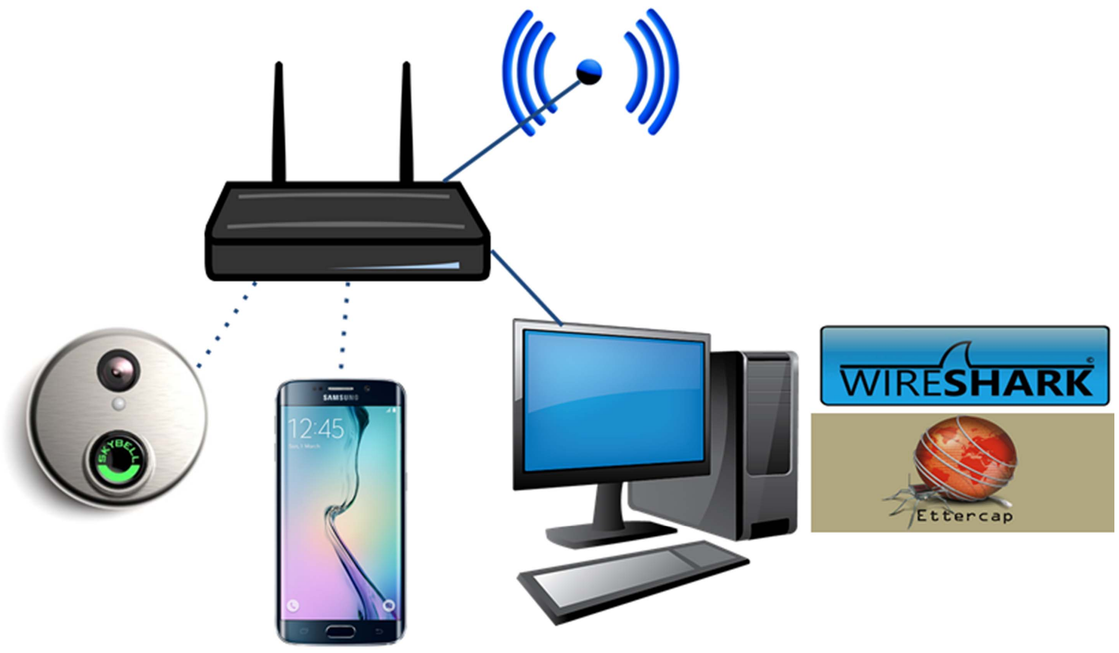

Figure 1: System Setup

Packet Length (Doorbell -> Aws)	CoAP Responses (Doorbell -> Aws)	Packet Length (Aws -> Doorbell)	CoAP Responses (Aws -> Doorbell)	Skybell Doorbell and App functionality
603		923		When Watch Live
987	4.04, , 4.08, GET	411	4.00, 4.08, PUT	When shifting from one AWS node to another Node
75	5.05	91	5.00	Hang up Call
491	4.02	891	GET	When connectivity is bad/ Bad Gateway
619	POST	907		Press watch live on Skybell app
507		363		When Skybell Doorbell button is pressed
		2 sets of 523	2.05	When Skybell Doorbell button is pressed for the first time without any other notification in hindsight
		976	ACK 2.05	Need to still figure out what this function is
		107	2.01	Need to still figure out what this function is

Table 1: Packets and Protocols led to identify what functionality was being performed

RESULTS

- 2 protocols used by the Skybell doorbell: CoAP (http://coap.technology) and RTCP (http://www.3cx.com/pbx/rtcp/")
- Skybell uses third party, Amazon Web Services.
- For each functionality of the Skybell, measured the five W: Who, When, Where, What and Why
- Using the captured data we were able to associate what data packets and protocols were used for specific functionalities and also able to figure out the CoAP responses as shown in Table 1.
- Knowing what functionality is being performed just by looking at the packets and protocols can be dangerous for the user because an injection attack can be performed on the doorbell whether it is using a video projection instead of the live stream video, or using a different voice to communicate through the doorbell

Confidentiality Test: In order to perform this test that data on Wireshark was checked to see if it was Encrypted or not. The data for all functionalities is not encrypted and hence **failed** the confidentiality test.
Integrity Test: To perform this test, IP Spoofing and Man in the Middle attack (MITM)-ARP Poisoning was used. Both the IP spoofing and the MITM attack allowed me to modify the information. Therefore, the integrity test **failed**.
Availability Test: In order to test this the Denial of Service attack was implemented. Denial of Service (DoS) Attack- Ping of Death the doorbell: An attack where a lot of ping packets are flooding from a source to the destination target IP Address which essentially makes the buffer overflow. This is done in-order to crash the device and make it unresponsive and is commonly known as the DoS attack**.** The doorbell failed the ping of death attack. Therefore, it **failed** the Availability test.

This research is a part of the Information Security Research and Education (INSuRE) project. INSuRE is a partnership between successful and mature Centers of Academic Excellence in Information Assurance Research (CAE-R) and the National Security Agency (NSA), the Department of Homeland Security and other federal and state agencies and laboratories to design, develop and test a cybersecurity research network. INSuRE is a self-organizing, cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project that can include both unclassified and classified research problems in cybersecurity.