I Spy Your Toaster: Cybersecurity and the Internet of Things

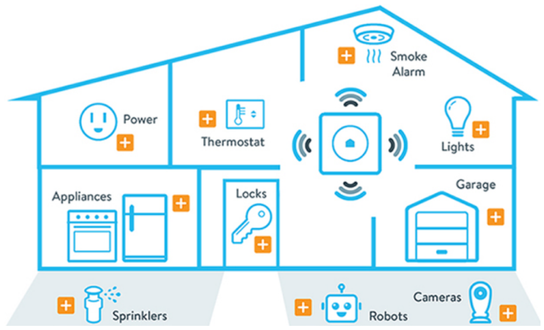
Celine Irvene, David Formby, Preethi Srinivasan, and Raheem Beyah
Communications Assurance & Performance Group
School of Electrical and Computer Engineering, Georgia Institute of Technology

Abstract

The network of Internet connected devices is rapidly expanding; from smart lights, to electronics locks, and even autonomous cars. This concept is known as the Internet of Things (IoT), and as the influence and prevalence of these devices continue to grow in society, so do the various security vulnerabilities associated with them. Users of IoT devices depend on them for raising the quality of life and increasing productivity, while ensuring the security and privacy of their data. Given the value and sensitivity of all the information that is at stake, there is a need for authentication of IoT devices. Currently, there is no effective way for fingerprinting IoT devices, but prior research has shown that device identification is possible on Industrial Control Systems (ICS), which are just larger scale Cyber Physical Systems (CPS). Using similar techniques, we were able to perform proof of concept device fingerprinting on a subset of Wink IoT devices. Wink is a company that develops software and devices for home automation, and the fingerprinting was performed on a smart LED light bulb and an intelligent window/door sensor.

Background

The Internet of Things is the concept of connecting any device with an on and off switch to the Internet and to each other. This includes everything from cell phones, coffee makers, washing machines, headphones, lamps, wearable devices, and just about anything else you can think of. The IoT is a giant network of connected “things”, with relationships from people-people, people-things, and things-things.



Motivation and Objectives

Motivation

In the home automation industry IoT devices are useful for to automating common tasks like turning on lamps, adjusting thermostats, and enabling coffee makers. To ensure privacy, IoT devices encrypt the communication between themselves and the IoT server, but that does not verify device identity. Fingerprinting will allow us to authenticate and identify devices so that we can differentiate between genuine and spoofed responses.

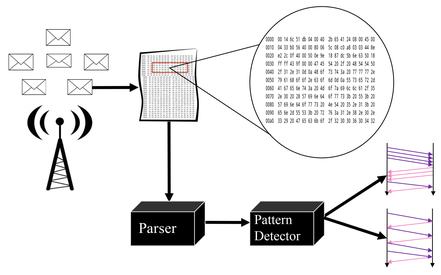
Objectives

- Learn how privacy is affected by IoT devices
- Discern how much information is leaked from IoT devices

Methodology

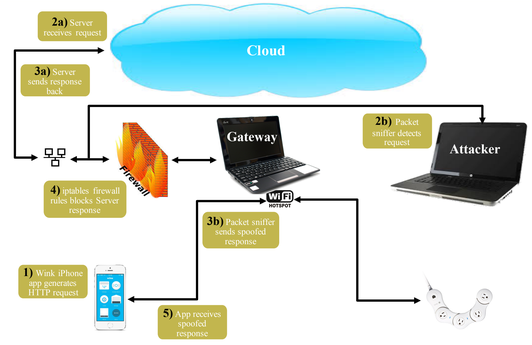
Reconnaissance

- Fingerprint Wink IoT devices using ZigBee protocol
  1. Collect and analyze network traffic for light and window/door sensor
  2. Identify packet sequence for light on command and sensor being triggered
- Developed Wi-Fi packet sniffer/parser
  1. Encountered encrypted network traffic
  2. Identified plaintext HTTP GET request



Launch Attack

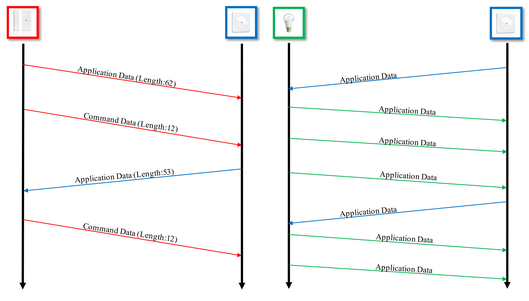
- Fuzzed Wink App
  1. Used sniffer to detect specific HTTP request packets from Wink App
  2. Crafted HTTP response packet with invalid data
  3. Sent invalid response to Wink App and blocked genuine response from the Wink Server



Results

Given encrypted ZigBee data capture

- Identify all devices on the network
- Determine whether a sensor was triggered
- Decipher if a light was turned on



Future Work and Conclusion

Future Work

- Expand number of known device signatures
- Design Wink API to control Wink IoT devices without use of the Hub
- Perform device characterization on Wink Wi-Fi devices

Conclusion

- This research has proven that device fingerprinting is possible for devices in the IoT
- We have also established that encryption does not ensure privacy