Exfiltration of Data Through Smart Light Bulb (IoT)

Mohammad Monjur and Pruthvy Yellu
Faculty Advisor: Prof Qiaoyan Yu
Department of Electrical and Computer Engineering, University of New Hampshire
Durham, NH 03824, USA

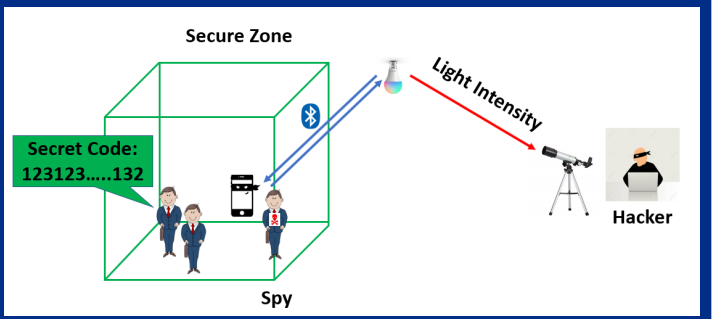
University of New Hampshire

Introduction

- Internet of Things (IoT) are connected to the network using many wireless technologies (Bluetooth and Zigbee etc.)
- Due to wireless nature most of the information is unsecured and are vulnerable to attacks.
- Attackers could breach the connection between IoT devices to leak information like secret code.

Attack Model

- Conman inside a secure zone with Bluetooth activation to stream real time information to smart bulb



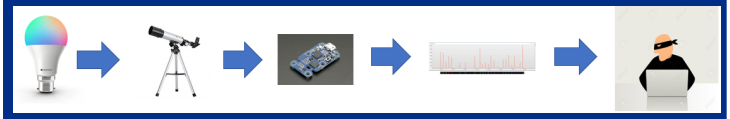
- Critical condition for the attack model
  - The room have mobile signal Jammer
  - Cellular frequency range 700MHz to 2000MHz
  - WLAN frequency range 2.4 GHz to 2.5 GHz
  - Smart bulb is outside of the secure zone
  - Light intensity change from a distance
  - Hacker encrypt the light intensity information

Attack Method

- Data exfiltration

Secret Number inside the room | Active the mobile app to capture real time value | Bluetooth data transmission | Smart Blue received the Bluetooth data outside

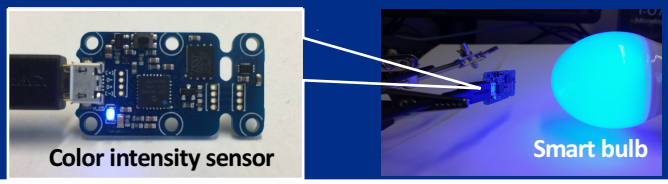
- Data decryption



Smart Blue received the Bluetooth data outside | lens to focus light on the sensor | Captured fluctuates luminance | Compare with library reference | Successfully decrypt the message

Experimental Setup

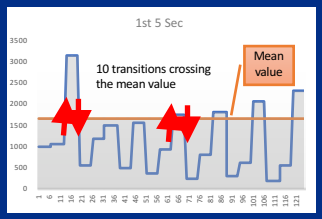
Setup for color intensity measurement

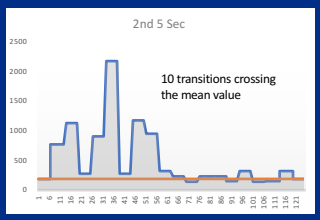


Experimental Results

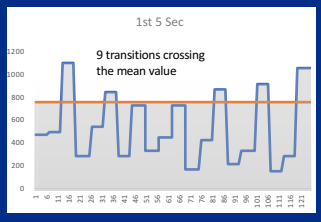
- Case study of a song

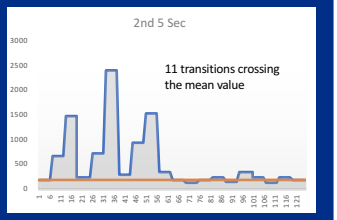
Trial 1 - Number of change compare to mean value are 20 in first 10 seconds





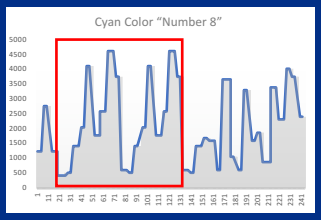
Trial 2 - Number of change compare to mean value are 20 in first 10 seconds

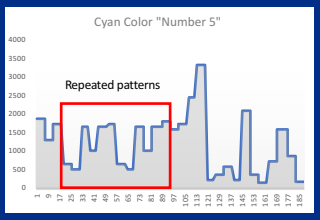




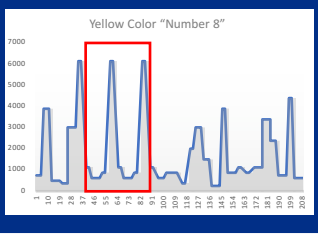
- Case study of numbers

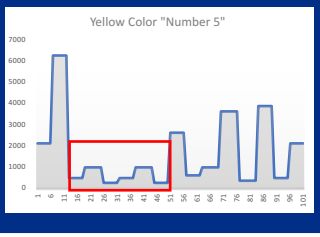
Stable patterns on cyan color measurement





Stable patterns on yellow color measurement





Conclusion

- This work demonstrate the potential security threats of the IoT devices.
- Transition pattern and color intensity are feasible side-channel signal to leak information in IoT devices.