A Security Assessment of Home Automation Systems

With the prevalence of Bluetooth Low Energy (BLE) and WiFi devices in the home, consumers must be aware of the information these devices inadvertently broadcast and what kind of privacy data an outside observer can infer without any network credentials. These protocols are increasingly used in a range of Internet of Things (IoT) devices such as security cameras, locks, and sensors. Two characteristics of IoT devices leave them vulnerable to data leakage: (i) these devices continuously broadcast unencrypted information, such as the Received Signal Strength Indicator (RSSI) and Media Access Control (MAC) address, which anyone with a properly-tuned receiver can observe, and (ii) the implementation of BLE security is left up to the developer and often results in essentially no link-layer authentication or encryption.

These vulnerabilities can be used to identify devices, track people’s movements, or deduce events such as when a door is opened or when a light is turned on. This paper presents how the raw signals and BLE vulnerabilities can be used to collect data from IoT devices without being connected to the smart home environment. It also observes what kind of information can be gathered and how an eavesdropper can use this data to identify users and create pattern of life models.

To demonstrate this, we developed a voice activated digital assistant and IoT architecture by integrating a variety of off-the-shelf WiFi and BLE devices with Apple's home automation application, HomeKit. Furthermore, we created an open-source pattern-of-life analysis tool and used other security tools to collect and analyze real IoT traffic. We also show how it is possible to piece together the sniffed information to track occupants of a house and crack a Bluetooth lock. Lastly, we present limitations to this approach and recommendations to prevent these vulnerabilities and create a more secure smart home environment.

This paper provides a unique method to identify and track devices within the smart home environment which ultimately allows eavesdroppers to create pattern of life models for users. This can be done without even connecting to the smart home environment via the raw signals sniffed over the air.