Through the looking glass: Exposing the vulnerabilities in smart doorbell systems

Claudia Rojas, Casimer DeCusatis, Pablo Rivas

Department of Computer Science and Mathematics, Marist College

Abstract

As the demand for home security grows many homeowners have begun to incorporate at least one Internet of Things (IoT) device in their home. While these devices provide homeowners peace of mind they also raise concerns about their reliability and security. IoT devices such as the smart doorbell systems are a major security concern in the cybersecurity community and they are the main focus of our research. Such IoT doorbell devices are popular in both homes and offices, and owners need to be aware of their security vulnerabilities. In this poster I will give an overview of the vulnerabilities in these devices to raise awareness of the current problems and the research opportunities they present.

Introduction

- The Internet of Things (IoT) has not been around for a long time, but it has evolved at an incredible pace.
- Steve Leibson stated that "The address space expansion means that we could assign an IPV6 address to every atom on the surface of the Earth and still have enough addresses left to do another 100+ Earths" [2].
- Cisco estimates that by 2020 there will be 50 billion devices in the IoT [3].
- The devices included in the IoT have become more prevalent in our everyday lives which brings up security and privacy concerns.
- Common security vulnerabilities include weak passwords, little or no data encryption, and insecure GUIs.
- Just these vulnerabilities alone can lead to major security breaches.
- Vulnerable IoT devices can be compromised by malware and be used as spam relays, cryptocurrency miners, and botnets, such as the Mirai botnet.

Background

- The main technologies we are using for this project are the Ring Video Doorbell Ver. 2, Nest Doorbell, and Skybell
- The WiFi feature in these devices are attractive to consumers because its easy to install and connect to them. This ease of use is a problem because it does not allow for strong encryption and weak security [1].
- One family's Nest camera was recently hacked and used to belt out a fake emergency message about an impending missile strike from North Korea using the Nest Cam's built-in speaker[5].

Approach

- This project looks into the security vulnerabilities identified from testing three smart doorbells currently on the market (Skybell, Ring, and Nest).
- Experiments include reconnaissance using port scans and man-in-the-middle attacks using a rogue access point to intercept the packets being transmitted.
- We will use hacking technologies readily available on the market such as the WiFi Pineapple Tetra, WireShark, and Aircrack-ng to penetrate the doorbell systems.

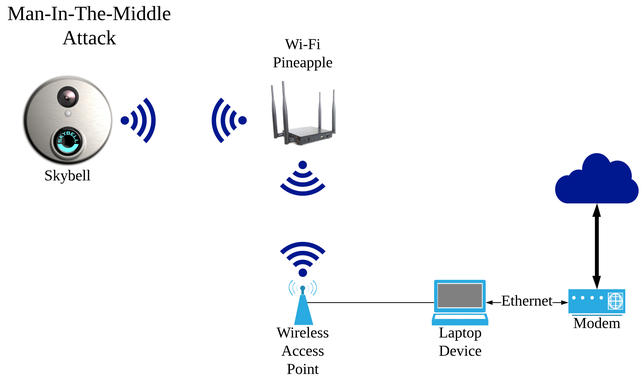

Fig.1. Network Diagram of the experimental setup for the Man-In-The-Middle attack on the Skybell device

Results

- We collected packets using the SiteSurvey module from the WiFi Pineapple Tetra and analyzed them with WireShark.
- Through the use of the WiFi Pineapple Site Survey module we were first able to find out information about the network(IOTLAB) all the devices are connected to.
  - Encryption: WPA2, Cipher: CCMP, Auth: PSK, Channel: 5, Frequency: 2.432
- Within this module we are able to deauthorize the devices on the network. The deauthorization attack disconnects the smart doorbells on the IOTLAB network and allows the WiFi Pineapple to capture the files being exchanged between the access point and the devices.
- Before deauthorizing the packets we collected multiple capture files to see what the devices were on the network.
- The capture files we collected were analyzed using Wireshark.
- The first few files we captured gave us information about the many devices one the network.
- We were able to find information on the Skybell such as its MAC address, encapsulation type(IEEE WLAN 802.11), and protocols in frame(wlan).
- We also found that the Ring is under the name as Texas Instrument by connecting the MAC address from the box the device comes in and from looking it up in Wireshark
- After we ran deauthorization to ensure that all the doorbell devices where disassociated from the network.
- We collected the files after we turned deauthorization on and off.
- By using this method we were able to collect the WPA keys for the Skybell and Ring as well as for a device using LGInnotek and Duratech.
- After finding the WPA key nonce for the Ring doorbell I was able to decrypt the keys using wireshark. By doing this I was able to find an IP address for the Ring doorbell and run an nmap scan.
- While we are only focusing on the smart doorbell devices we also found smart plugs that were unprotected

```
NSE: Script scanning [redacted]
Initiating NSE at 19:00
Completed NSE at 19:00, 0.00s elapsed
Initiating NSE at 19:00
Completed NSE at 19:00, 0.00s elapsed
Nmap scan report for Ring.lan [redacted]
Host is up (0.0095s latency).
All 65535 scanned ports on Ring.lan [redacted]
are closed
MAC Address: [redacted] (Unknown)
Too many fingerprints match this host to give specific
OS details
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   9.52 ms Ring.lan [redacted]

NSE: Script Post-scanning.
Initiating NSE at 19:00
Completed NSE at 19:00, 0.00s elapsed
Initiating NSE at 19:00
Completed NSE at 19:00, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any
incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 780.77
seconds
           Raw packets sent: 67380 (2.967MB) | Rcvd:
66172 (2.663MB)
```

SamsungE_35:f2:29	Skybell_08:1b:a2	EAPOL	133	Key (Message 1 of 4)
Skybell_08:1b:a2	SamsungE_35:f2:29	EAPOL	155	Key (Message 2 of 4)
SamsungE_35:f2:29	Skybell_08:1b:a2	EAPOL	189	Key (Message 3 of 4)
Skybell_08:1b:a2	SamsungE_35:f2:29	EAPOL	133	Key (Message 4 of 4)

206	-0.000016		Skybell_08:1b:a2 (d0:c1:93:08:1b…	802.11	10	Clear-to-send, Flags=........
207	-0.000001	SamsungE_35:f2:29 (2c:ba:ba:35:f2:29)…	Skybell_08:1b:a2 (d0:c1:93:08:1b…	802.11	28	802.11 Block Ack, Flags=........
208	0.003601	Skybell_08:1b:a2 (d0:c1:93:08:1b:a2) …	SamsungE_35:f2:29 (2c:ba:ba:35:f…	802.11	28	802.11 Block Ack, Flags=........
209	0.001024	Skybell_08:1b:a2 (d0:c1:93:08:1b:a2) …	SamsungE_35:f2:29 (2c:ba:ba:35:f…	802.11	16	Request-to-send, Flags=........
210	0.012784		Skybell_08:1b:a2 (d0:c1:93:08:1b…	802.11	10	Clear-to-send, Flags=........
211	0.000000	SamsungE_35:f2:29 (2c:ba:ba:35:f2:29)…	Skybell_08:1b:a2 (d0:c1:93:08:1b…	802.11	28	802.11 Block Ack, Flags=........
212	0.793131		1c:f2:9a:c3:ee:f1 (1c:f2:9a:c3:e…	802.11	10	Acknowledgement, Flags=........
213	0.002050		1c:f2:9a:c3:ee:f1 (1c:f2:9a:c3:e…	802.11	10	Acknowledgement, Flags=........

```
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03
19:03 Eastern Daylight Time
Nmap scan report for Ring.lan [redacted]
Host is up (0.010s latency).
All 1000 scanned ports on Ring.lan [redacted] are
closed
MAC Address: [redacted] (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 9.83
seconds
```

References

[1] Lewis, James A. Managing risk for the Internet of Things. Washington: Center for Strategies & International Studies, 2016.
[2] Foote, Keith. "A Brief history of the Internet of Things." Dataversity, https://www.dataversity.net/brief-history-internet-things/
[3] Evans, Dave. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. San Jose: Cisco Internet Business Solutions Group (IBSG), 2011
[4] Chang, Lulu. "A Ring doorbell vulnerability lets people snoop even after a password change." Digital Trends, https://www.digitaltrends.com/home/ring-video-doorbell-security-exploit/
[5] Gafni, Matthias. ""5 minutes of sheer terror": Hackers infiltrate East Bay family's Nest surveillance camera, send warning of incoming North Korea missile attack." The Mercury News. https://www.mercurynews.com/2019/01/21/it-was-five-minutes-of-sheer-terror-hackers-infiltrate-east-bay-familys-nest-surveillance-camera-send-warning-of-incoming-north-korea-missile-attack/