SmartHome Security

Addy Moran
Kyle Haefner

Problem Description

SmartHome devices are connected primarily through Wi-Fi; if a hacker gains access to the consumer's Wi-Fi network they could view video feeds, passwords and other personal information, and they could change settings that make the SmartHome unsafe. How would a home owner keep their information secure? How can someone protect against common device and Wi-Fi vulnerabilities?

Common SmartHome Vulnerabilities & Exploits

Wi-Fi

Process (WPA/WPA2)

1. Find available networks and monitor target Wi-Fi
2. Send a de-authorization packet to target
3. Capture WPA handshake
4. Compare handshake to a wordlist

Security Cameras

Process (D-Link Device)

1. Monitor port 24
2. Use Hydra to Brute Force D-Link log in page to gain access to live feed and settings.

What they can do?

- View live camera feed
- Change settings for audio, video, can change times when system is looking for motion

Wi-Fi Protected Setup (WPS)

Overview

- Uses a PIN to authenticate access
- Vulnerable to Brute Force Attacks which allows hackers to try all possible PIN numbers until the correct one allows the hacker to gain access to the victims network

Process

- Use Reaver to brute force 4 digits - some routers use two concatenated 4 digit pins with the last digit being a checksum
  - total options = 4 digits + 3 digits = $10^4 + 10^3 = 11{,}000$
  - time: can be done in two hours

General SmartHome Information

Platform

SmartHomes commonly use a main hub to control other devices in the Smart Home. The main hub and the devices are connected to the consumer's network. This allows the consumer easy access to all the devices in one place; however this also causes security vulnerabilities that hackers can exploit.

Devices & the Internet

- The number of Wi-Fi connected devices could be anywhere between 50 – 75 billion by 2020.
- A typical home could have more than 500 smart devices by 2022.
- Some devices are required to be on Wi-Fi to operate with full features (Xbox One).

Common Applications

- Entertainment: SmartTV, Sound System, Game Systems
- Security: Security Cameras, Electronic Locks, Motion Detectors
- Kitchen: Smart Fridge, Smart Slow Cooker
- Utilities: Thermostat, Water Manager, Smoke/C02 Detectors

Exploitation Videos

Resources

Potential Protective Measures

Wi-Fi

1. Have a safe password
2. Change wireless network name (SSID) which helps prevent hackers from knowing which network is which
3. Filter MAC addresses
4. Make your Wi-Fi range smaller

Security Cameras

1. Have a safe password
2. Change default settings (username, password, device name)

SmartHome

1. Use a safe router, change default password, and update firmware frequently
2. Use a cloud service to help manage devices
3. Use authentication and access control measures for all devices
4. Update devices

Safe Passwords

1. Don't use dictionary words
2. Make passwords at least 12 characters
3. Include special characters, numbers, and a mixture of upper and lower case characters
4. Don't use obvious substitutions

* Word and password lists are common ways hackers * get access to Wi-Fi, accounts, and devices.

Conclusion

SmartHomes have devices that are connected through Wi-Fi networks and have vulnerabilities which make them susceptible to hacker activities. Hackers may gain virtual and physical access and cause irreparable damage. SmartHomes and their devices should improve their security and safety features to allow home owners an enhanced lifestyle experience seamlessly.

07/31/2016

Poster Presentation