HackBerryFi

Home IoT Devices Security Assessment

Objective

Analyze a set of home IoT devices currently sold in the market to assess their security and determine if the users of this kind of devices are being exposed to risks that they ignore.

Additionally, finding vulnerabilities on the devices can help to create security awareness on the manufacturers and alert their strategic managers about the products that are being sold.

Motivation

The use of home IoT devices is increasing with each day that passes. Users acquire them without any knowledge of the security risk that the devices might bring to their sensitive information or privacy. Our hypothesis as the HackBerryFi team is that the security of such devices is not good enough. Manufacturers that do not take security seriously need to be exposed to protect people's privacy and sensitive data.

Methodology

The security assessment was done by understanding thoroughly the functionality of the devices by doing reverse engineering on each their components. Additionally, dynamic and static analysis, both manual and automated, was done to find vulnerabilities. The vulnerabilities found by automated tools were tested manually to eliminate the high number of false positives reported by automated means.

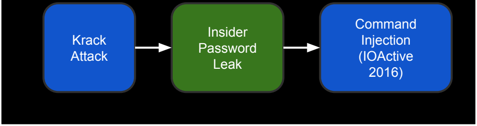
Devices and vulnerabilities

Uniden Appcam 23

- **Logged secrets exposed**
  a. Wifi password
  b. Authentication password
  c. Configuration commands
- **Easy DoS**
  a. hping3 tool successful Dos on single laptop
  b. Authentication password
- **Use of HTTP**
  a. Insecure firmware update
  b. Insecure email configuration

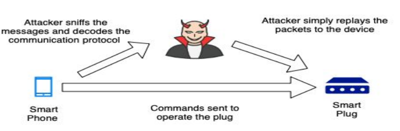
TP Link Camera

- Pinned certs for all remote connections
- Reverse TCP connection to bypass NAT
- Broken internal authentication protocol
- Vulnerable to SYN Flood DOS attack



TP link HS100 Smart plug

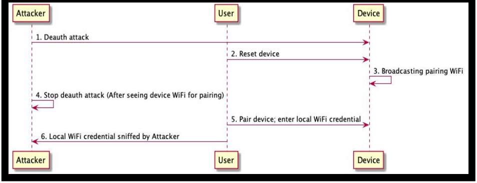
- Weak Encryption in transit messages
- Most MiTM attacks prevented due to certificate pinning
- Replay attack possible as the requests sent from the mobile app to the plug do not have:
  a. Authentication tokens
  b. Random nonce
  c. Strong encryption



Attacker sniffs the messages and decodes the communication protocol
Attacker simply replays the packets to the device
Smart Phone
Commands sent to operate the plug
Smart Plug

WeMo Smart Plug

- Pairing protocol
- Unencrypted WiFi
- Deducible decryption key: SN + MAC
- Encryption: AES CBC
- Distinguishable device: OUI
- All WeMo wireless IoT device affected



Attacker
User
Device
1. Deauth attack
2. Reset device
3. Broadcasting pairing WiFi
4. Stop deauth attack (After seeing device WiFi for pairing)
5. Pair device; enter local WiFi credential
6. Local WiFi credential sniffed by Attacker
Attacker
User
Device

Recommendations

Uniden Appcam 23

Install digital Certificate on every server that interacts with the application.
Use SYN Cookie to prevent DOS.
Add code review process to catch output of sensitive information

TP Link Camera

TCP SYN cookie
Authentication token
Encrypted traffic

TP Link HS100 Smart Plug

Implement Authentication token
Access controls
Replay resilience
Freshness tokens

WeMo Smart Plug

Encrypted WiFi with randomly generated password
User experience versus security

Moving Forward

- More rigorous firmware level analysis
- Physical penetration testing (SPI, UART, JTAG)
- Reversing the iOS applications of the 4 devices