The Secret Life of IoT Devices: A Security Analysis

Junia Valente, Alvaro A. Cardenas | The University of Texas at Dallas

Introduction

We analyze over a dozen of Internet of Things (IoT) devices, and summarize vulnerabilities we found on them:

(1) encryption problems on a smart toy,
(2) filesystem misconfigurations on consumer drones, and
(3) hard-coded passwords on camera firmware.

We show proof-of-concept attacks and techniques we used.

Note: We reported the vulnerabilities we found to CERT/CC & affected vendors following a responsible disclosure approach.

Approach

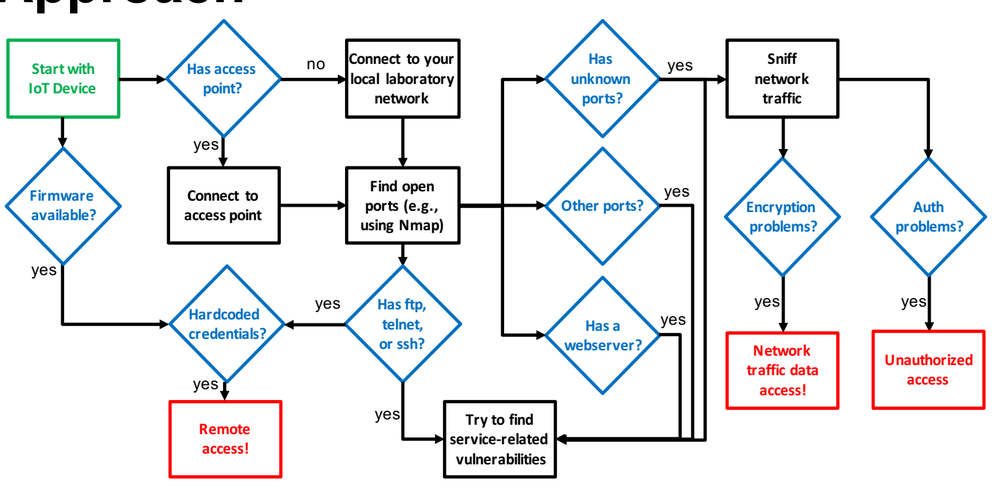

Figure 2. Our proposed steps to perform vulnerability assessment on IoT devices.

In this poster, we focus our discussions to:
(1) firmware analysis
(2) network running services analysis
(3) network traffic analysis (e.g., device <-> cloud)
(4) authentication/authorization issues

Our recent contributions: CVE-2017-3209, CVE-2017-8865/66/67.

Overview

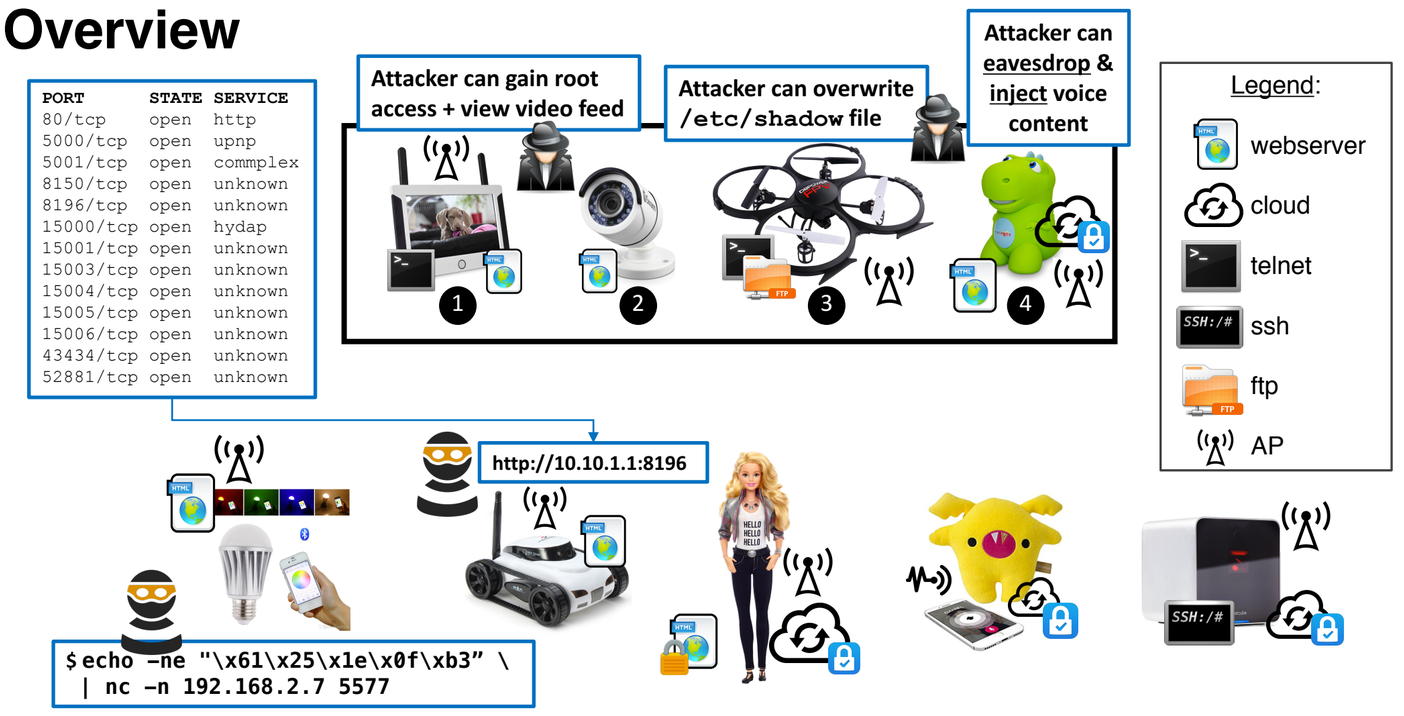

Figure 1. Example of consumer IoT devices we have in our lab.

Security Analysis of Security Cameras

We discovered and reported vulnerability [3]: **CVE-2015-8287**

```
[03:30:15] jvalente: binwalk nvr-firmware.pak

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
36989         0x907D          Certificate in DER format (x509 v3), header length: 4, sequence length: 1280
90812         0x162BC         CRC32 polynomial table, little endian
174741        0x2AA95         Certificate in DER format (x509 v3), header length: 4, sequence length: 1280
258124        0x3F04C         CRC32 polynomial table, little endian
425248        0x67D20         uImage header, header size: 64 bytes, header CRC: 0x73D9C2E7, created: 2014-12-08
06:37:01, image size: 2823708 bytes, Data Address: 0x80008000, Entry Point: 0x80008000, data CRC: 0xD6E9FF38,
OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none, image name: "Linux-2.6.37"
442003        0x6BE93         gzip compressed data, maximum compression, from Unix, last modified: [...]
3249020       0x31937C        CramFS filesystem, little endian, size: 8597504 version 2 sorted_dirs CRC [...]
11846524      0xB4C37C        CramFS filesystem, little endian, size: 10969088 version 2 sorted_dirs CRC [...]
22815612      0x15C237C       PC bitmap, Windows 3.x format,, 684 x 456 x 24
23751378      0x16A6AD2       CramFS filesystem, little endian, size: 4096 version 2 sorted_dirs CRC [...]
```

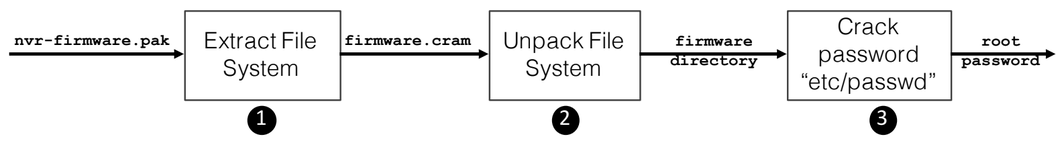

Figure 3. Extracting root password---hard-coded---in the firmware.

Security and Privacy for Drones

We discovered and reported vulnerability: **CVE-2017-3209**

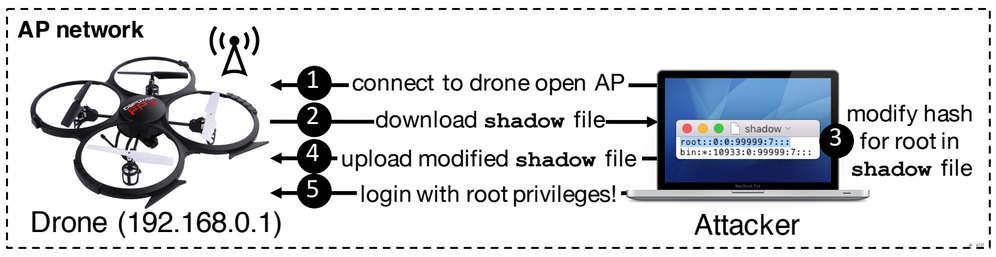

Figure 4. A near-by attacker can modify sensitive files (via a mis-configured anonymous ftp login) to gain root access via Telnet.

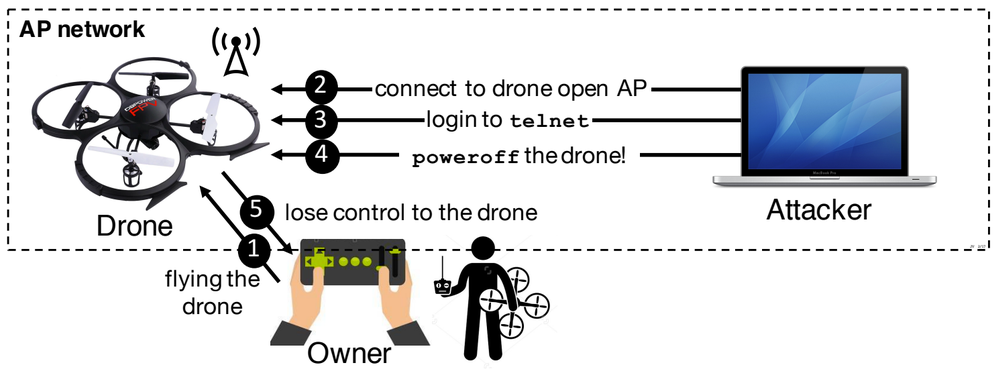

Figure 5. A near-by attacker can take down a flying drone via the Telnet access (from the previous attack).

Internet Connected Smart Toys

An attacker can **(1) listen** what a child speaks to their toy; and can **(2) inject voice** content to a child's toy [4]

Steps (simplified):

1. Attacker captures **traffic** between a dino and cloud
2. Attacker replays **traffic** to another dino device!

An attacker can make:
Dino toys speak arbitrary things to a child:

→ Ask child to open front door
→ Insult the child

We discovered and reported several vulnerabilities: **CVE-2017-8867**, **CVE-2017-8866**, and **CVE-2017-8865**.

(1) Dino devices use **weak mode of encryption**
(2) Dino devices use **hard-coded keys** for encryption
(3) Dino devices are vulnerable to **replay-attacks**

Figure 6. List of vulnerabilities we found & attacks we tested on CogniToys Dino.

Discussion and Conclusion

We show that voice-enabled toys---targeting young children---pose new unanticipated threats [4]. An attacker can inject malicious voice content and insult or ask young children to do unsafe things. Also, an attacker can obtain private-sensitive data (when the toy is lost or resold). We successfully tested these attacks.

Further, we tested a variety of attacks in a new family of drones (U818A) released in 2016 [1, 2]. Our concerns over safety (taking down a drone operated by someone else) and privacy (taking unauthorized pictures) alert us that even when a drone is purchased as a toy, cyber-attacks can have dangerous, real-world consequences [5].

Reference

[1] C. Brook, Many Commercial Drones Insecure by Design. Threatpost Security News, May 2017.

[2] CERT/CC, Note VU#334207 - DBPOWER U818A WIFI quadcopter drone allows full filesystem permissions to anonymous FTP, 2017.

[3] CERT/CC, Note VU#923388 - Swann SRNVW-470 allows unauthorized access to video stream and contains a hard-coded password, 2016.

[4] J. Valente and A. Cardenas, Security & Privacy of Smart Toys, IoT S&P at CCS'17, 2017.

[5] J. Valente and A. Cardenas, Understanding Security Threats in Consumer Drones Through the Lens of the Discovery Quadcopter Family, IoT S&P at CCS'17, 2017.

THE UNIVERSITY OF TEXAS AT DALLAS
Erik Jonsson School of Engineering and Computer Science

ACKNOWLEDGEMENTS: This material is based upon work supported by Air Force Office of Scientific Research under award number FA9550-17-1-0135 and by NSF under award number CNS 1553683.