Security Analysis of Consumer IoT Devices

Junia Valente, Alvaro A. Cardenas
The University of Texas at Dallas
{juniavalente, alvaro.cardenas}@utdallas.edu

Introduction

Internet of Things (IoT) devices are found everywhere, including in our homes, in healthcare, in education, and for entertainment.

As our lives become more dependent on these systems, their security and privacy practices is a growing concern.

This poster summarizes our study of security practices in a variety of consumer Internet of Things (IoT) devices [1-4] & proposes new sensor-assisted security protections against various attack strategies [5].

Sample of Consumer IoT Devices We Have in Our Lab

Figure 1. IoT devices we considered

Approach

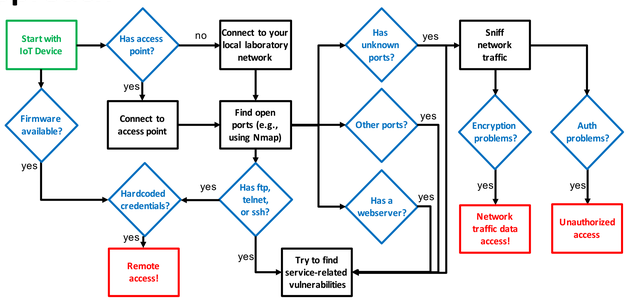

Figure 2. Our proposed steps to perform vulnerability assessment on IoT devices.

Internet-Connected Smart Toys [2]

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 door
→ Insult the child

Figure 3. Attacks we tested on CogniToys Dino based on vulnerabilities we found on the device.

An attacker can **(1) listen** what a child speaks to their toy; and can **(2) inject voice** content to child's toy (even when there is encryption) due to vulnerabilities we found on the device

We discovered CVEs: `CVE-2017-8867/66/65`.

Security Analysis of Cameras [4]

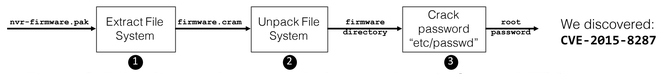

Figure 4. Extracting root password---hard-coded---in Swann NVR firmware.

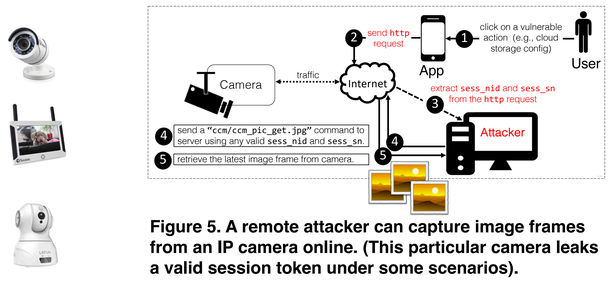

Figure 5. A remote attacker can capture image frames from an IP camera online. (This particular camera leaks a valid session token under some scenarios).

Study of Drones [3]

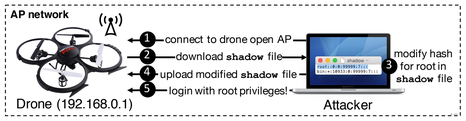

Figure 6. A near-by attacker can modify sensitive files (via a mis-configured anonymous ftp login) to gain root access via Telnet.

A near-by attacker can take down a flying drone (from the Discovery family of drones) via the Telnet access

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

Visual Challenge Proposal for Cameras [5]

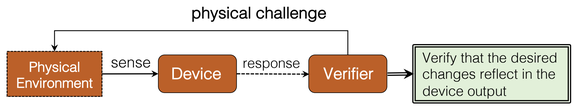

Figure 7. New sensor-assisted security protections.

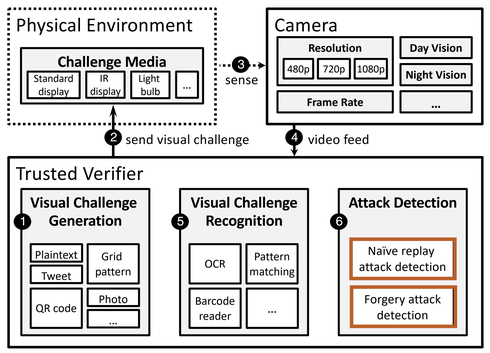

Figure 8. We extend our previous proposal to support new visual challenges such as a grid pattern of IR LEDs and use multi-color smart light bulbs to change ambient lighting.

Figure 9. Multi-color smart light challenges.

Figure 10. People cannot see the infrared challenge.

Figure 11. Cameras with night vision can see IR visual challenges.

Conclusion and Future Directions

Our systematic analysis identifies security practices & trends of IoT devices. We hope our work can be useful in evaluating future IoT (e.g., Industrial IoT) security proposals by showing common pitfalls in available technologies. We propose new tools to detect tampering of video feeds from security cameras.

	Comm. to cloud?	Connectivity type	AP (initial setup)	AP (persistence usage)	AP security	WiFi provisioning	webserver (port 80 or diff port)	ftp (port 21)	telnet (port 23)	ssh (port 22)	unknown/other tcp ports	Firmware update	Operating System
❶ Swann 470LCD (NVR)	✓		◐	◐ or ✗	WPA2	n/a or ⌑	✓		✓●		✓	⟲	Linux 2.6.37
❷ Swann 470CAM (camera)	✓⁺		✗	✗	n/a	n/a or ⌑⁺	✓				✓✓	✗?	–
❸ Petcube Play Pet Camera	✓		○	✗	none	🔊 (🅱 or)	✓			✓●	✓	⊞ or ⟲	DD-WRT v24 or v30
❹ LeFun Baby Monitor	✓		✗⁺	✗	n/a	♪ or ✂, or n/a	✓				✓	⟲	–
❺ I-SPY Mini tank	✗		◐	◐	WPA2	n/a	✓				✓✓✓✓	✗?	Linux 2.6.30.9
❻ IJR/C H49 mini drone	✗		○	○	none	n/a			✓○		✓	✗	RT-Thread OS 2.0.1
❼ DBPOWER U818A drone	✗		○	○	none	n/a		✓○	✓●		✓✓✓	✗	Linux 3.4.35
❽ Force1 U818A drone	✗		○	○	none	n/a		✓○	✓●		✓✓	✗	Linux 3.4.35
❾ Parrot AR Drone 2.0	✗		○	○	none	n/a		✓○	✓○		✓✓✓	⟲	Linux 2.6.32.9
❿ CogniToys dino	✓		○	✗	none	🔊 ()	✓					⊞	–
⓫ Toymail Talkie	✓		✗	✗	n/a	✂						⊞	–
⓬ Hello Barbie	✓		○	✗	none	🔊 ()					✓	⊞	–
⓭ Wemo smart plug	✓		○	✗	none	🔊 ()					✓✓	⟲	Linux 3.18
⓮ EDIMAX smart plug	✓		○	✗	none	🔊 ()	✓					⟲	Linux 2.6.x
⓯ MagicLight	✓		○	✗	none	🔊 ()	✓				✓	✗?	–
⓰ OZOM Box	✓		●	✗	WPA2	n/a	✓			✓●	✓	⊞	Linux 2.6.x/3.x
⓱ VeraEdge hub	✓		●	● or ✗	WPA2	n/a or 🔊 ()	✓			✓●	✓✓	⟲	Linux 3.10.34
⓲ SmartThings hub	✓		✗	✗	n/a	n/a					✓✓	⊞	DD-WRT v24 or v30
⓳ Amazon Echo Dot	✓		○	✗	none	🔊 ()	✓				✓✓	⊞	Google Android 4.1.x
⓴ Amazon Echo	✓		○	✗	none	🔊 ()	✓				✓✓	⊞	Linux 2.6.x
㉑ Google Home	✓		○	✗	none	🔊 ()	✓				✓✓✓	⊞	Linux 2.6.x/3.x
㉒ Bellabeat health tracker	✓⁺		✗	✗	n/a	n/a						⟲	–
㉓ UNICEF Kid Power	✓⁺		✗	✗	n/a	n/a						✗?	–

Legend: ○ open, ◐ common password (e.g., '1234'), ● strong password, ✗ no Access Point (AP) (or not applicable);
Firmware update ⊞ automatic, ⟲ manual, ✗ no firmware update, ✗? unclear how (if possible),
✍ according to manual (i.e., not to our observations); ⁺ via another device (e.g., ✓⁺ communication or ⌑⁺ input);
WiFi provisioning via physical (i.e., ♪ sound, ✂ visual) or 🔊 digital channel, or ⌑ manual input on device screen;
Number of unknown or other ports: ✓ (1-2 ports), ✓✓ (3-4 ports), ✓✓✓ (5-6 ports), ✓✓✓✓ (7 or more ports);
Connectivity type: WiFi, Ethernet, Zigbee, Z-Wave, Bluetooth; "–" represents *no exact OS matches.*

Table 1. Summary of Security Practices in the 23 IoT devices we considered.

Reference

[1] J. Valente, M. Wynn, and A. Cardenas (2019). Stealing, Spying, and Abusing: Consequences of Attacks to Internet of Things Devices. IEEE Security & Privacy, vol. 17, no. 5.

[2] J. Valente and A. Cardenas (2017). Security & Privacy of Smart Toys. ACM IoT S&P at CCS'17.

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

[4] J. Valente, K. Koneru, and A. Cardenas (2019). Privacy and Security in Internet-Connected Cameras. IEEE Congress on Internet of Things (ICIOT'19).

[5] J. Valente, K. Bahirat, K. Venechanos, A. Cardenas, and P. Balakrishnan (2019). Improving the Security of Visual Challenges. ACM Transactions on Cyber-Physical Systems (TCPS'19).

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

ACKNOWLEDGEMENTS: This material is based upon work supported by the Air Force Office of Scientific Research under award FA9550-17-1-0135, by NSF under award CNS 1553683, and by the Laboratory for Analytic Sciences (LAS). Any opinions, findings, conclusions, or recommendations expressed are those of the authors and do not necessarily reflect the views of the sponsors and / or any agency of the United States Government.