Testing/Analysing IoT devices for vulnerabilities

Andrew Watson - Supervised by: Konstantinos Markantonakis
Information Security Group, Smart Card and IoT Security Centre

The Smart Card and Internet of Things Security Centre

Objectives

To research current IoT security trends and perform practical investigative security testing/analysis of the CCTV DVR class of IoT devices.

Specifically:
- Enumerate devices for potential vulnerabilities
- Prove exploitability of discoveries
- Provide analysis of results in terms of potential impact, highlighting common vulnerabilities
- Discuss prevention and mitigation of security issues discovered
- Explore practical options for enhancing security including implementing non native security services.

Introduction

IoT is a rapidly expanding technology connecting previously offline embedded devices to the Internet.

Data released by the research company Gartner [1] estimate that connected IoT devices exceed:
- Current - 6 Billion
- By 2020 - 20 Billion.

Millions of the IoT devices deployed contain security vulnerabilities and are being exploited on a massive scale by hackers and malware. Mirai and BASHLITE [2] IoT botnets are responsible for some of the largest cyber attacks ever, including the 2016 Dyn DNS DDoS.

The real world impact of exploited IoT devices ranges from relatively little to life threatening, as devices with known vulnerabilities include:
- Smart Locks
- Internet routers
- CCTV cameras & DVR's
- Cars
- Pacemakers & Insulin pumps.

Internet security practices are mostly transferable to IoT in theory, but in some cases security best practice does not scale to IoT. This is due to multiple factors such as IoT specific requirements for low power/cost. Therefore a new approach is required to enhance native IoT security to meet best practice.

Testing Lab Setup

Specific hardware & software was configured to create a testing lab required for the practical research.

Lab environment:
- Kali Linux OS
- Kali integrated security testing tools
- CCTV DVR IoT devices
- Client devices
- Network protocol/packet analyser
- Man-in-the-middle (MITM) device
- Managed switch with port mirror
- Ancillary networking services
- IoT Proxy proof of concept security solution.

Methods

Testing scope was defined based on:
- Default 'out of the box' IoT security configuration
- Tested from the perspective of an Internet based attacker knowing only an IP address
- No other knowledge of the device other than what can be established remotely.

Enumeration was carried out in two stages:
- General device and service agnostic scans for a high level map of network services/potential vulnerabilities
- Fine tuning of general scan output into device and service specific enumeration.

Testing actioned all enumeration results to execute IoT device specific attack vectors and prove exploitability with proof of concept.

Important Results

None of the devices tested offer transport encryption for any remote connections, brand new CCTV DVR vulnerable to 15 year old DoS exploit, remote OS root access gained, and multiple insufficient password protection protocols.

PoC Code

Figure 1 below shows a proof of concept exploit created to leverage a 15 year old Denial of Service vulnerability discovered in a brand new all-in-one CCTV DVR IoT device. The script sends 10 incomplete HTTP requests which results in the DoS condition.

```
#!/bin/bash
# Script written by Andrew Watson for MSc Project.
# Exploits Denial of Service condition
# Payload source: www.exploit-
db.com/exploits/21939/
#
echo "DVR Denial of Service - 10 connections"
for dos in $(seq 1 10); do
echo "DoS Connection: $dos sent!"
#payload:
perl -e 'print "GET " . "/" . " HTTP/1.1\r\n"' |
netcat 192.168.1.19 5000 &
#end payload
done
```

Figure 1: Proof of Concept Denial of Service exploit.

Results

Device	Potential Vulnerabilities	Proven Vulnerable	Not Vulnerable	False Positive	Out of Scope
DVR 1	15	9	1	1	4
DVR 2	7	3	0	0	4
DVR 3	6	2	1	0	3
DVR 4	9	1	1	4	3
TOTAL	**37**	**15**	**3**	**5**	**14**

Table 1: High level vulnerability results.

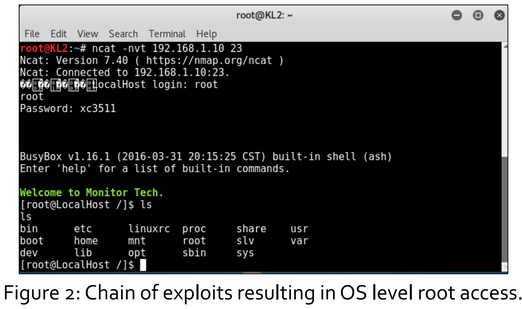

Figure 2: Chain of exploits resulting in OS level root access.

Conclusion

The IoT devices tested are not secured to industry best practice and cost has little relation to default security. None offered any form of encryption on remote access services, free to fix vulnerabilities were not corrected and DoS/password protocol failures were discovered in multiple devices. Considering that CCTV provides physical security these results have real world impact.

Additional Information

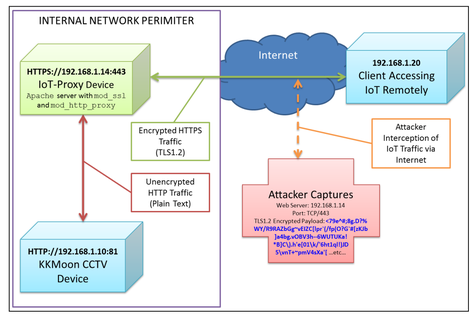

Figure 3: IoT Proxy Proof of Concept adding TLS1.2 encryption.

References

[1] R. van der Meulen
Gartner Newsroom, 10/11/2015
http://www.gartner.com/newsroom/id/3165317
[2] P. Paganini
BASHLITE Botnets peaked 1 Million IoT Devices, 01/09/2016.
http://securityaffairs.co/wordpress/50824/malware/bashlite-botnets.html

Acknowledgements

Steve Wakeland @ ITSO
Konstantinos Markantonakis @ RHUL
Fred Piper @ RHUL
Ken Munro @ Pen Test Partners

Contact Information

- Web: https://keybase.io/bitfu
- Email: Andrew.Watson.2015@rhul.ac.uk
- Phone: +44 (0)1784 414409