Digging Deep: How to Find and Exploit Bugs in IoT Devices

Kelvin WONG
Speaker@

- SANS DFIR Summit
- DFRWS EU
- HTICA US
- DefCON 20
- HITCON
- CodeBule
- AVTokyo
- APWG
- ISC² APAC Congress

ISLA (Asia Pacific) 2016 Honoree
Publications

» 10 years experience in Digital Forensics
» Facebook Forensics (2011) on Hakin9 Magazine
» Mac Memory Forensics (2014) on Digital Forensics Magazine
» Investigation and Intelligence Framework (2015) on Forensics Focus
» Advanced Mobile Devices Analysis Using JTAG and Chip-Off (2016) on eForensics Magazine
Hacking IoT?
Attack Vector on IoT

» Ecosystem
» Device Memory
» Device Physical Interfaces
» Device Web Interface
» Device Firmware
» Etc... (OWASP IoT project)
Protocol / Software based

» Wifi
» BLE
» Zigbee
» RF
» NFC
» HCE
Hardware Based?
13.2 (S) Firmware Inspection

(S) To be able to inspect a firmware image that is loaded on a device, an adversary would need to disassemble the device, solder a JTAG header onto the board, and extract the firmware from the flash chip through the JTAG using JTAG extraction software. The team has been able to successfully solder a JTAG and extract the firmware from a Linksys WRT54G.
Hardware based method?

» UART
» JTAG
» ISP
» Chip-off
JTAG

» Joint Test Action Group
» Communicate with memory chips through Test Access Ports (TAPs)
» Physical data acquisition
» Have different pins
Test Access Port (TAP)

» TCK – test clock
» TMS – test mode state
» TDI – test data in
» TDO – test data out
» TRST – test reset
» NRST – normal reset
» RTCK – return clock
» GND – ground
Linksys Router JTAG pins
UART

» serial communications over a computer or peripheral device serial port

» Transmitting and receiving serial data

» See the output from console
UART pins

Serial port 1 (ttyS0)

Serial port 2 (ttyS1)

2: 3.3V
4: TX 0
6: RX 0
8: NC
10: GND

3.3V - 1
TX - 1 - 3
RX - 1 - 5
NC - 7
GND - 9
BusBlaster

Attify

Etc.......
OpenOCD

» Open Source
» Open On-chip Debugger tool
» Provide debugging, in system programming and boundary-scan test
» Work with a list of debug adapter
» Support a list of router/chips configuration
Chriss-MacBook-Pro-3:openocd Chris$ openocd -f interface/MyBlaster.cfg
Open On-Chip Debugger 0.10.0+dev-00131-g3414dae (2017-05-05-13:07)
Licensed under GNU GPL v2
For bug reports, read
http://openocd.org/doc/doxygen/bugs.html
Info : If you need SWD support, flash KT-Link buffer from https://github.com/bhari
and use dp_busblaster_kt-link.cfg instead
adapter speed: 1300 kHz
Info : clock speed 1300 kHz
Info : JTAG tap: bcm5352e.cpu tap/device found: 0x0535217f (mfg: 0x0bf (Broadcom
), part: 0x5352, ver: 0x0)
Info: If you need SWD support, flash KT-Link buffer from https://github.com/rissau/busblaster and use dp_busblaster_kt-link.cfg instead
adapter speed: 1300 kHz
Info: clock speed 1300 kHz
Error: JTAG scan chain interrogation failed: all zeroes
Error: Check JTAG interface, timings, target power, etc.
Error: Trying to use configured scan chain anyway...
Error: bcm5352e.cpu: IR capture error; saw 0x0 not 0x1
Warn: Bypassing JTAG setup events due to errors
^C
Chriss-MacBook-Pro-3: openocd ChrisS openocd -f interface/MyBlaster.cfg
Open On-Chip Debugger 0.10.0+dev-00131-g3414dae (2017-05-05-13:07)
Licensed under GNU GPL v2
For bug reports, read
http://openocd.org/doc/doxygen/bugs.html
Info: If you need SWD support, flash KT-Link buffer from https://github.com/rissau/busblaster and use dp_busblaster_kt-link.cfg instead
adapter speed: 1300 kHz
Info: clock speed 1300 kHz
Info: JTAG tap: bcm5352e.cpu tap/device found: 0x0535217f (mfg: 0x0bf, part: 0x5352, ver: 0x0)
Info: accepting 'telnet' connection on tcp/4444
Kill the watchdog and halt system
Print the kernel address value
**Magic Header of Kernel Section**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>magic number</td>
<td>'HDR0'</td>
</tr>
<tr>
<td>length</td>
<td>header size + data</td>
</tr>
<tr>
<td>32-bit CRC</td>
<td>value</td>
</tr>
<tr>
<td>TRX flags</td>
<td></td>
</tr>
<tr>
<td>TRX version</td>
<td></td>
</tr>
<tr>
<td>Partition</td>
<td>offset[0]</td>
</tr>
<tr>
<td>Partition</td>
<td>offset[1]</td>
</tr>
<tr>
<td>Partition</td>
<td>offset[2]</td>
</tr>
</tbody>
</table>
Memory Dump

» firmware-recovery script from Openocd
» Image_dump (If address do not match)
» CFE Memory: 0x9fc00000, size: 0x40000
  KERNEL Memory : 0x9fc40000, size: 0x1B0000
  NVRAM Memory : 0x9fDF0000, size: 0x10000
Whole FLASH structure

» Common Firmware Environment (CFE) - bootloader

» Kernel - firmware

» NVRAM - store variable information
Secret

» Plaintext username and password

» No authentication is required for console login

» RAM address: 0x80000000 size: 0x01000000
ISP – In System Circuit Programming
Amazon Alexa
Chip-Off
Google Home Mini
Chip-off Village by VXRL
VXCON on 21-22 April in Hong Kong
Discount code for HITB AMS

‘hitb@ams_@vxcon2018’
https://www.eventbrite.hk/e/vxcon-2018-tickets-43644511910
Or www.vxcon.hk for agenda

Thank You!