IOT HARDWARE HACKING - DEMOING FIRMWARE EXTRACTION AND PROTECTION METHODS

Deral Heiland
Research Lead (IoT)
Rapid7
@percent_x

Nathan Sevier
Senior Security Consultant
Rapid7
@__r4ge__
Agenda

- Why is hardware security important?
- How is hardware security compromised?
- What security methods are available for prevention?
WHY

Hardware security is important
Protecting intellectual property
Why

Mitigate and protecting brand reputation

“It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you'll do things differently.”

--Warren Buffett--
Protect against device compromise

```
root@LWR-1370:/etc# whoami
root
root@LWR-1370:/etc# uname -a
Linux LWR-1370 4.4.26-yocto-standard #1 PREEMPT Fri Nov 11 17:19:18 UTC 2016 armv7l GNU/Linux
root@LWR-1370:/etc# cat /etc/shadow
root:7MKEFKR3iw06:17367:0:99999:7:::
bubba:7MKEFKR3iw06:17367:0:99999:7:::
daemon:*:17367:0:99999:7::
```
HOW

Demo examples of device compromise and firmware extraction
Extracting Memory Chips

- Destructive
- Flash
  - SPI
  - NAND/NOR
  - eMMC
- Demo
Gaining Root Access Via UART

- Bypass authentication
- U-Boot console
  - Interrupt boot cycle
  - Alter boot arguments
- Live Demo
WHAT

Methods available for improving security
What

- Secure boot
  - Authenticated against the hardware
  - Required signing to execute on MCU
  - Prevent tampering
• Built in processor flash protections

<table>
<thead>
<tr>
<th>FWDREN</th>
<th>ON</th>
<th>Watchdog Timer Enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1FC0_2FFC</td>
<td>OFF</td>
<td>Background Debugger Enable</td>
</tr>
<tr>
<td>DEVCFG0</td>
<td>OFF</td>
<td>ICE/ICD Comm Channel Select</td>
</tr>
<tr>
<td>ICS_PGx2</td>
<td>OFF</td>
<td>Program Flash Write Protect</td>
</tr>
<tr>
<td>PWP</td>
<td>OFF</td>
<td>Boot Flash Write Protect bit</td>
</tr>
<tr>
<td>BWP</td>
<td>OFF</td>
<td>Code Protect</td>
</tr>
</tbody>
</table>
What

- Disable
  - UART
    - Disabled in production
  - JTAG
    - Disable in Production
      - Electronic fuse
      - Physical fuse
What

- Encryption firmware & data
  - Storage
  - Transmission
  - Trusted Platform Module (TPM)