IoT: A security hole without a patch

Earl Carter
Senior Threat Researcher
Agenda

- State of IoT
- Security Implications
- Averting Disaster
Connection Craze

What could possibly Go Wrong?
20 Billion Connected Devices by 2020

Security Holes

Security Holes Everywhere
Security Implications?

World's Biggest Mirai Botnet Is Being Rented Out For DDoS Attacks

Mirai botnet attack hits thousands of home routers, throwing users offline

Germany's federal security office confirmed that almost a million customers in the country were affected by internet outages as a result of the attack.

By Zack Whittaker for Zero Day | November 29, 2016 -- 07:00 GMT (23:00 PST) | Topic: Security
Security Implications?

Smart Locks Used by Airbnb Get Bricked by Software Update

Rhett Jones
Monday 6:39pm • Filed to: IOT FAILURES

A DEEP FLAW IN YOUR CAR LETS HACKERS SHUT DOWN SAFETY

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY WITH ME IN IT

FDA finds St. Jude Medical cardiac devices can be hacked

Wi-Fi baby heart monitor may have the worst IoT security of 2016
What do the Pro’s say
Real Life Example

- Rob Joyce Chief, Tailored Access Operators NSA
  - “..there’s even the heating and cooling systems”
- Talos identified several flaws in Trane ComfortLink II thermostats and alerted Trane to them in April 2014.
Vulnerability Details

- CVE-2015-2867 - Hardcoded credential vulnerability
- CVE-2015-2868 - Buffer overflow flaws leading to remote code execution

```
def exploit
    lop = 
        0xeaffffe
    .pack('V')

    xor = 
        0xe28f7018, # add r7, pc, #24
        0xe3a06078, # mov r6, #120 ; 0x78
        0xe3a04088, # mov r4, #136 ; 0x88
        0xe7d73006, # ldrb r3, [r7, r6]
        0xe0233004, # eor r3, r3, r4
        0xe7c73006, # strb r3, [r7, r6]
        0xe2566001, # subs r6, r6, #1
        0x5afffffa # bpl c <.text+0xc>
    .pack('V*')
```
Why pop IoT?

- Where are the advisories?
- download the update -
Advisories?

```
.o0( craiwill@CRAIWI-LL-X-0D3 temp ) tar zxf rsup_145007844901.tar.gz
```

- a_145007844901
- b_145007844901
- c_145007844901
- d_145007844901
- e_145007844901
- f_145007844901
- g_145007844901
- v_145007844901
- m_145007844901
Advisories?

```
$ (craiwill@CRAIWILL-M-G0D3 temp ) head m_145007844901
<version_info>
<product build='145007844901' release='4.0.3' date='14-Dec-2015' downloadSize='90922', installationSize='95468'>
<features>
<feature notes='Improved WiFi management, Comm Bus improvements'/>
</features>
<fixes>
<fix info='Security fixes, courtesy: Cisco Talos'/>
<fix info=' Improved comm link reporting with 940'/>
</fixes>
<checksum></checksum>
```

![Shocked Kid]
Foscam Cameras

- Talos Identified over 20 0-days (patched in June)

- Query Append Buffer Overflow Vulnerability
- Account Password Command Injection Vulnerability
- FTP Hard Coded Password Vulnerability
- Wifi Settings Code Execution Vulnerability
- NTP Server Configuration Command Injection Vulnerability
- Multi-part Form Boundary Code Execution Vulnerability
- SMTP Test Command Injection Vulnerability
LOL - Best Practices?

Figure 3.60

Enter the User name and password

CAUTION: If your camera works well with the current firmware, we recommend not upgrading. Please don’t upgrade the firmware unnecessarily. Your camera may be damaged if misconfigured during an upgrade.
Averting Disaster

Who thinks about patching their IoT devices?
Where are the advisories?
Many updates are firmware fixes.
Some devices can’t even be updated.
Where are ASLR & DEP?

Community Actions
Pressure Vendors on Security
Don’t blindly deploy IoT
Segment devices on the Network
Where will we end up?

Crisis
Averted

QA Called
Your Code Failed