IoT BBQ
Carve Systems

Outline

- About us (Carve)
- About IoT
- Our IoT assessment methodology
- The Sacred Tenants of IoT Security
- Some bugs
- IoT IRL

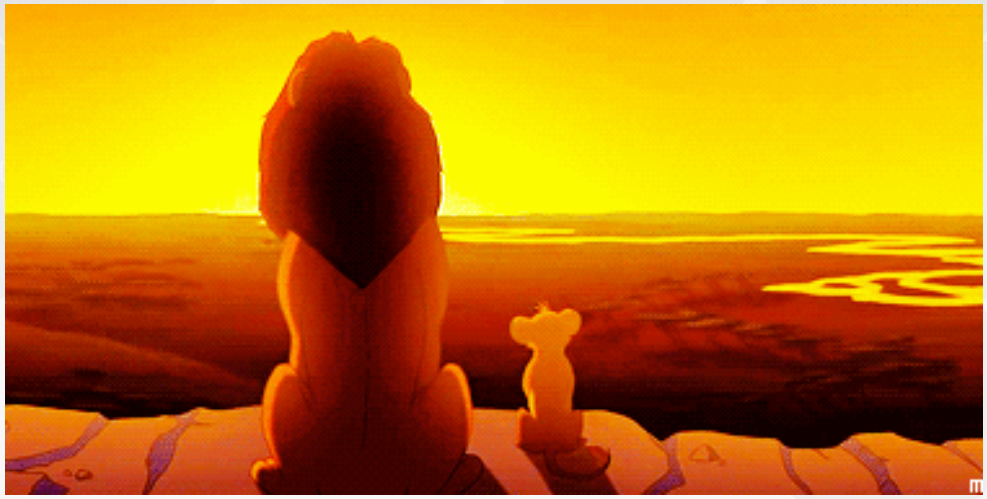
0xGROG

- Carve Systems
  - Boutique Information Security Consulting Firm
  - Clients in Denver!
  - Full stack hacking
- Jeremy Allen – Partner
  - See the future, make research happen
- Max Sobell – Partner
  - Find shiny things, bang them with rocks
- Carve team: we're all here!

Artwork by Mike Ferrin

OWASP
Open Web Application Security Project

What is IoT BBQ?



- Home automation/security
- SMB connectivity
- Municipal
- WTFThings
- Everything the internet touches

What exactly is “IoT”

- Things
- On the Internet
- The same things that have been there the whole time
  - Embedded Systems
  - M2M

“IoT is insecure!”

- Everyone knows it. Literally everyone. Even my old neighbors.

```
10 SOUND ALARM
15 REM ALARM IN PROGRESS
20 ???
30 PROFIT
40 GOTO 10
```

How IoT is Marketed

SHINY

IoT Reality

IoT Device Profile

Primarily embedded systems (Linux)

16 – 512MiB RAM Common

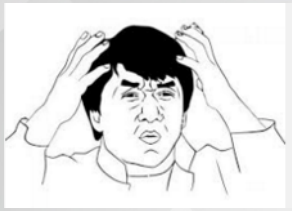
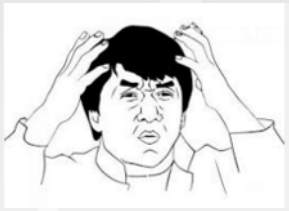
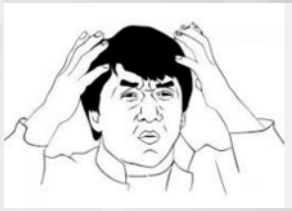
2-8 GiB Flash Storage Common

ARM Processors, Occasional X86 or MIPS

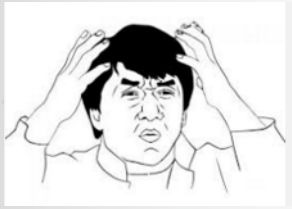
Internet Connected

Most have a management web application

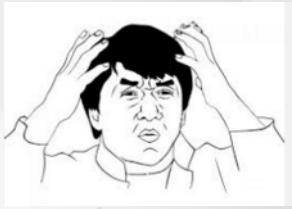
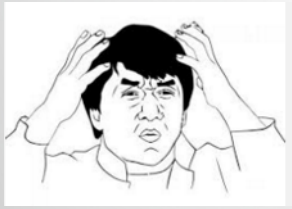
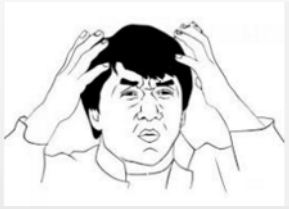
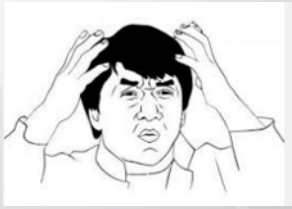
IoT Hardware vs. Software

Embedded Systems / Hardware developers tasked with creating software:



"I know C. Let's just write everything as CGI scripts in C. Oh, and maybe a bash script when I am feeling bold. That should create a management app that meets the requirements."

IoT Software

- We've seen:
  - Web servers that let you "PUT" server-side scripts to set/reveal admin passwords
  - Countless command injections to root
  - Janky encryption routines that can be broken in practice
- First sacred tenant of Secure IoT development:

Don't re-invent the wheel

Odd command injection

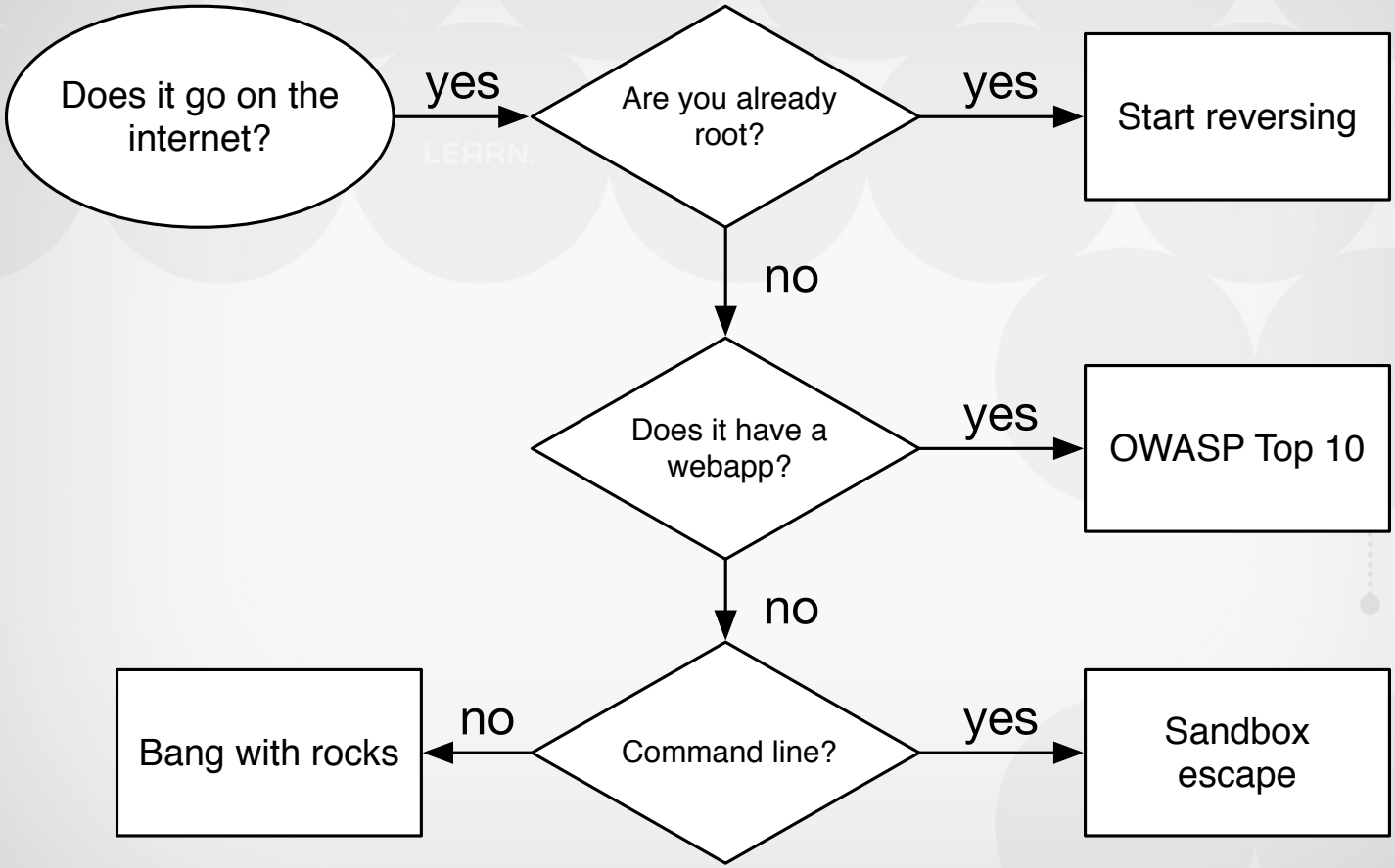
- Ruggedized Router/Vehicle Tracker
- This thing has it all:
  - Web app flaws (auth bypass, command injection)
  - Insecure default settings
  - Awful cryptography
  - Way too easy to shoot yourself in the foot

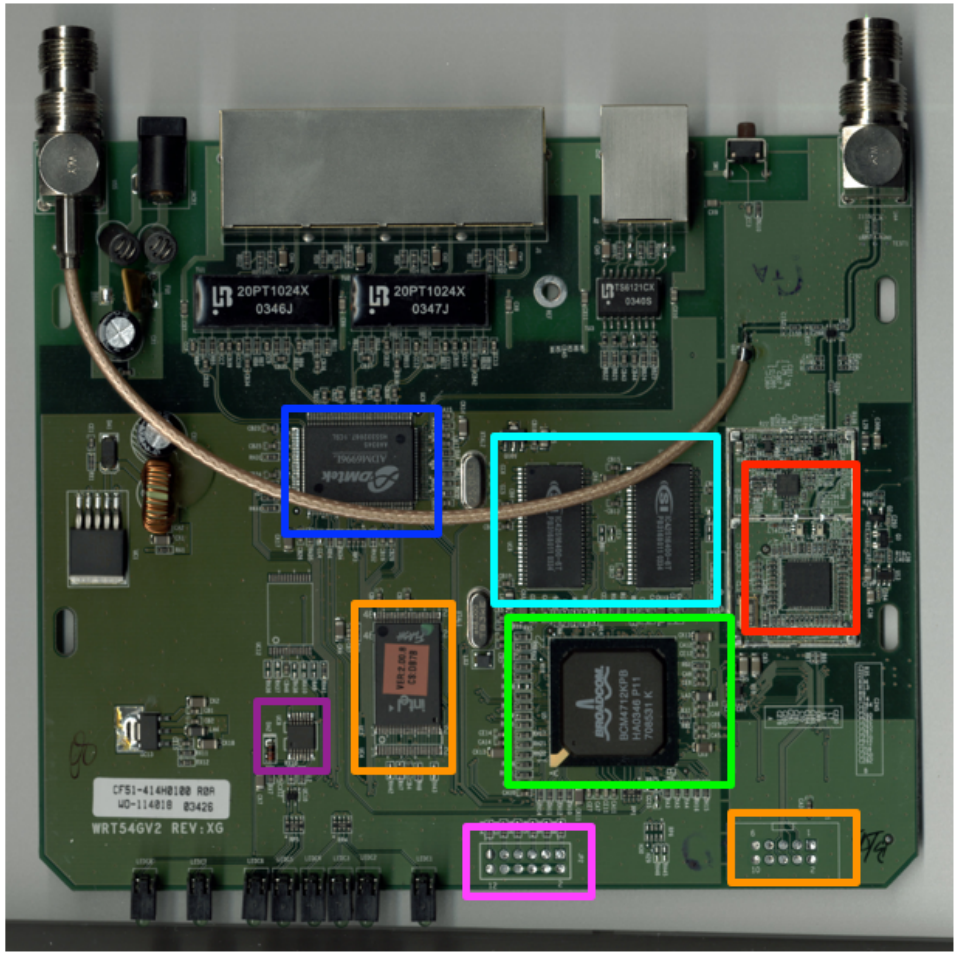
<demo video>

How do impactful bugs happen?

- The goal: using what you know about your device, get root on another device
- Start with the admin
  - How do they configure the device?
  - How do they monitor/interact?
- Can you download a firmware image?
  - Is the file system easy to mount and work? Encrypted?

IoT Methodology Cheat Sheet




20PT1024X
0346J
20PT1024X
0347J
WRT54GV2 REV:XG

Step by step: root

- Assume the user is root
- Why would you already be root?
  - It's your device
  - If you're not already root, you will be shortly
- Second sacred tenant of IoT development:

Secrets from one device should not be shared with other devices

No sharing

- Don't trust these devices for a second
  - Privileged network access
  - Hard-coded keys (encryption, SSH)
  - Backdoor accounts
  - Updating
- Public case study #1: Updating

How doth one update?

- Home alarm system
  - Android
  - No web app, no admin config
  - No problem
- Dealer network
- Force-browse to the update package

CVE-2015-6032, 6033; https://www.kb.cert.org/vuls/id/573848
Thanks, CERT!

Via SD Card

SOFTWARE UPDATE VIA SD CARD

To perform a software update using an SD Card:

Obtain an SD card with at least 1GB of free space.
Login to Dealers.Qolsys.com and locate the software update on the "Downloads" page.
Save the file onto your SD card.
Slide the SD card into the slot on the back left of the par
Touch "Settings" and enter your installer code

dealers.qolsys.com/media/qolsys-downloads/Software-downloads/

Index of /media/qolsys-downloads/Software-downloads

- Parent Directory
- 12518SD.zip
- SD-1.zip
- SD-2.zip
- Software-Patch-131.zip
- Software-Patch-132.zip
- Software-Patch-134.zip
- Software-Patch-141.zip

Apache Server at dealers.qolsys.com Port 80

Name	Date Modi		
data.tar.gz	Dec 16, 2		
release.txt	Dec 16, 2		
system	Dec 18, 2014, 2:34 PM	--	Folder
system.tar.gz	Dec 16, 2013, 7:32 PM	78 MB	GZip archive
zImage.tar.gz	Dec 16, 2013, 7:33 PM	3.4 MB	GZip archive

Oh no…

```
public FileTransfer(Context paramContext)
{
  SharedPreferences localSharedPreferences = PreferenceManager.getDefaultSharedPreferences(paramContext);
  this.mContext = paramContext;
  this.hostName = localSharedPreferences.getString("SERVER_NAME", "[redacted]7.249").trim();
  if ("".equals(this.hostName))
    this.hostName = "[redacted]7.249";
  this.userName = localSharedPreferences.getString("USER_NAME", "ubuntu").trim();
  if ("".equals(this.userName))
    this.userName = "ubuntu";
  this.password = localSharedPreferences.getString("PASSWORD", "[redacted]").trim();
  if ("".equals(this.password))
    this.password = "[redacted]";
  this.port = localSharedPreferences.getString("PORT", "22").trim();
  if ("".equals(this.port))
    this.port = "22";
  String str = localSharedPreferences.getString("WORKING_DIRECTORY", "").trim();
  if (("".equals(str)) || ("/".equals(str)))
  {
    setWorkingDir("/home/ubuntu/sftp/");
    return;
  }
  setWorkingDir("/home/ubuntu/sftp/" + str + "/");
}
```

OWASP
Open Web Application Security Project

Private signing key

```
Romans-MacBook-Pro:raw roman$ /Library/Java/JavaVirtualMachines/jdk1.8.0_20.jdk/
Contents/Home/bin/keytool -list -v -keystore iqma.bks -storetype BKS -providercl
ass org.bouncycastle.jce.provider.BouncyCastleProvider  -storepass iqolsys

Keystore type: BKS
Keystore provider: BC

Your keystore contains 1 entry

Alias name: iqolsys
Creation date: Jul 2, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: C=US,ST=CA,L=SunnyVale,O=QolSys Softwares,OU=Software,CN=QolSys
Issuer: C=US,ST=CA,L=SunnyVale,O=QolSys Softwares,OU=Software,CN=QolSys
Serial number: 53b3e4d2
Valid from: Wed Jul 02 06:54:10 EDT 2014 until: Sun Nov 17 05:54:10 EST 2041
Certificate fingerprints:
         MD5:  98:C9:D3:C1:FD:B9:4F:8A:F2:A8:6C:08:D9:8D:0E:8A
         SHA1: CF:BA:2E:1B:9A:2D:F3:85:FD:97:AD:B0:55:61:79:AC:B0:E1:97:E9
         SHA256: 16:94:2A:9A:E1:B0:FD:B8:0B:14:3B:02:23:EE:BC:95:68:B0:29:30:F4:
74:39:3A:AD:AB:AD:07:3C:C7:D0:01
         Signature algorithm name: SHA1WITHRSA
         Version: 3
```

Attack scenario

- Attack scenario:
  - Create malicious update package
  - Sign with vendor private key
  - Log in + push update to vendor server [we did not try this]
  - All devices download malicious update package and install (key matches) [or this]
- This bug is now fixed – thanks to CERT for coordinating disclosure

CERT FTW

Vulnerability Summary for CVE-2015-6032

Original release date: 10/31/2015

Last revised: 11/02/2015

Source: US-CERT/NIST

Overview

Qolsys IQ Panel (aka QOL) before 1.5.1 has hardcoded cryptogra

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 HIGH

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

Vulnerability Summary for CVE-2015-6033

Original release date: 10/31/2015

Last revised: 11/02/2015

Source: US-CERT/NIST

Overview

Qolsys IQ Panel (aka QOL) before 1.5.1 does not verify the digital signa

Impact

CVSS Severity (version 2.0):

CVSS v2 Base Score: 9.3 HIGH

Vector: (AV:N/AC:M/Au:N/C:C/I:C/A:C) (legend)

Impact Subscore: 10.0

Exploitability Subscore: 8.6

CVSS Version 2 Metrics:

Access Vector: Network exploitable

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized disclosure of information; Allows unauthorized modification; Allows disruption of service

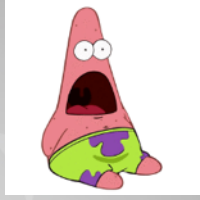
More on CERT

- They run a great service
- We prefer to disclose bugs to CERT first
- CERT will help coordinate disclosure if the vendor becomes unresponsive
  - (or if the world is going to end)
- They will **only** publish if they coordinate disclosure

CS CARVE SYSTEMS

Artwork by Mike Ferrin

OWASP
Open Web Application Security Project



We want more bugs!

- IoT fixes are **slow**. Not our timeline*:

DISCLOSURE TIMELINE

2014-04-09 - Initial contact with Trane is established. Advisories delivered.
2014-06-03 - Second attempt to contact Trane for follow up. No response received.
2014-08-15 - Third attempt to made to contact Trane for follow up. No response received.
2014-09-30 - Fourth attempt to contact Trane is made. Advisories re-sent. No further correspondence.

- Slow to patch. Slow to update.

```
$ _x='() { echo vulnerable; }' bash -c '_x 2>/dev/null || echo not vulnerable'
vulnerable
$
```

- We'll see shellshock until the end of time.

*http://blog.talosintel.com/2016/02/trane-iot.html

Who cares?

- Apart from getting your WiFi password from your doorbell, why should you care?
  - Privileged network access
  - Corporate secrets (passwords)
  - Sensitive data (location)

http://thehackernews.com/2016/01/doorbell-hacking-wifi-pasword.html

Things, as far as the eye can see

- Target of opportunity
- Also likely the weakest point in a chosen target
- Attacker can:
  - Exploit device directly as a foothold
  - Use device's routing to get to corp network
  - Siphon off device secrets and try them elsewhere

IoT Use Cases

- Centralized management of connected things
- IoT devices enable:
  - Connectivity
  - Convenience
  - “Can I control it from my phone?

Abuse Cases

- Access to privileged networks (including your home)
- Convenience undermines security
- IoT devices themselves are not the prize
  - Contain sensitive data
  - Live in privileged net segments

What to do

- Eliminate bad trust relationships: what I do has no effect on others.
- Patch bugs! Lots of software re-use
- Fail closed
- Secure defaults
- Implement the 80% hardware security controls
- Don’t re-invent the wheel

Contact

Email: {info,jeremy,max}@carvesystems.com

Twitter: @bitexploder, @msobell

http://carve.systems

Thank you OWASP and conference organizers!