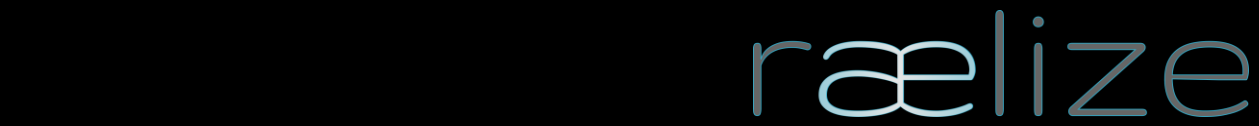


The Hidden Threat: Breaking into Connected Devices for Infrastructure Compromise

Cristofaro Mune
cristofaro@raelize.com
@pulsoid

Introduction.

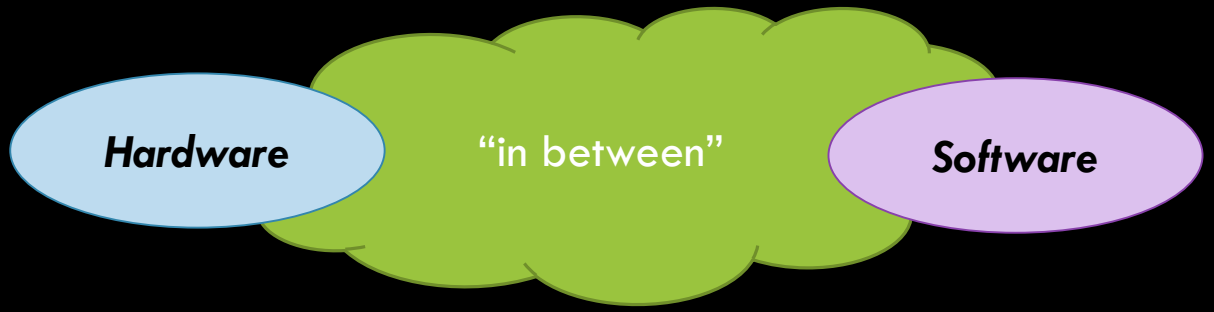
Me

Cristofaro Mune

- Co-Founder at Raelize; Security Researcher
- 20+ years in security
- 15+ years analyzing the security of complex systems and devices

ræ lize

- Based in The Netherlands. Specialized in Device Security
- Security testing, Consultancy and Training
- Low level software, hardware security:
  - Secure Boot, TEE, Fault injection,…



Our research: https://raelize.com/blog

Goals

- Discuss security of modern devices
- Demonstrate how *"Devices **ARE** endpoints"*
- Show threats they may introduce
- Assess impact: ***Enterprises*** and ***Critical infrastructures***
- Check effectiveness of established IT security practices
- Share insight from product security to reduce risks and exposure

Raise awareness

Agenda

- Current IT security status ← → Device security
- Setting our scenarios:
  - Enterprises and Critical infrastructures
- Attack gallery. A sequel of (live) demos to:
  - Demonstrate device-based attacks
  - Provide opportunity for reflection:
    - Prevention, Detection, Mitigation, Response
- Hint to next-generation attacks
- Recommendations and closing considerations

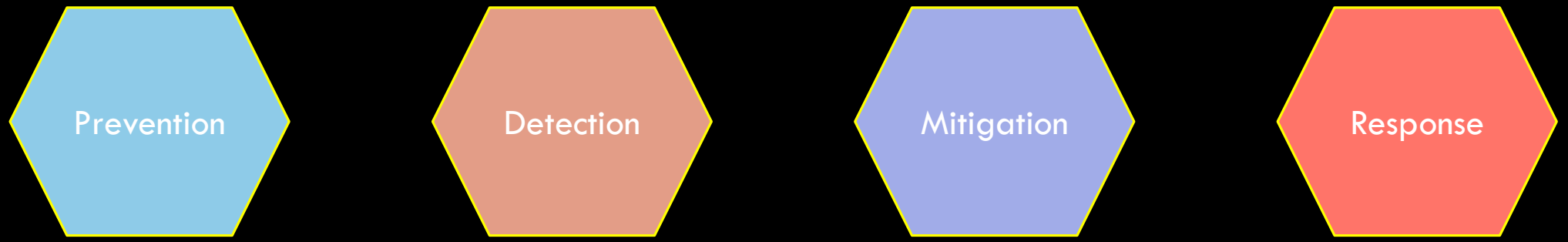
A (very) quick dive in IT security.

A few notable events

- Morris worm (1988):
  - Computer security becomes a topic
- TCP Wrapper by Wietse Venema (1992)
  - The first "firewall". Network security comes alive
- Aleph One – "Smashing the stack for fun and profit" (1996)
  - First (publicly known) write-up of stack overflow exploitation. Exploitation becomes public.
- Windows-based worms (Code Red, Nimda,…) (2001):
  - We discover ecosystem-level impacts of vulnerabilities
- Security marked as "top-priority" at Microsoft (2002)
  - Paves the way for some software security practices

IT Security: Nowadays

- Focuses on software
- Mostly evolved in the context of "Enterprise Security"



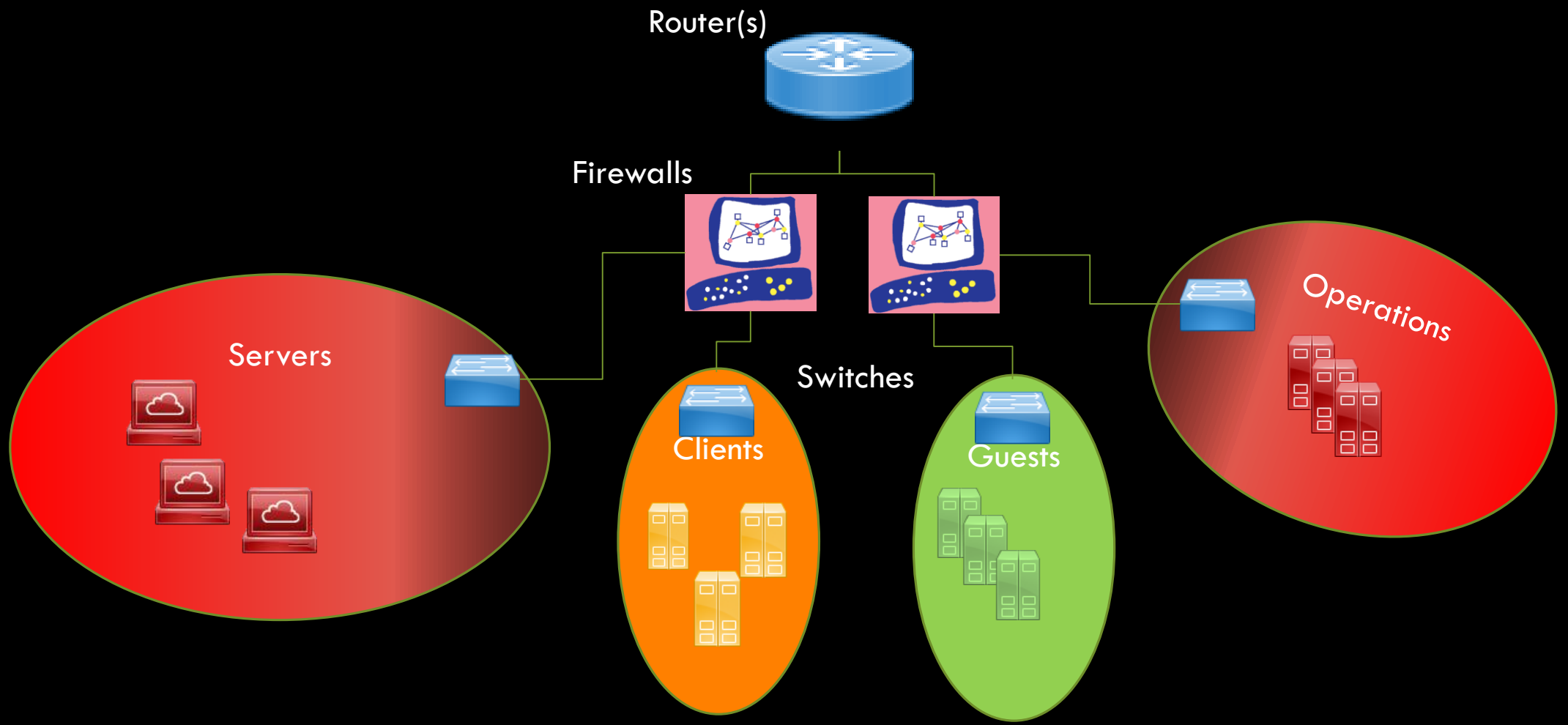
- Development:
  - Secure-SDLC
  - Defense-in-depth
- Testing:
  - PT, VA, Red/Blue/Purple teaming
  - …

- SOC
- SIEM,
- WAF
- EDR/XDR,
- …

- Network segregation
- Privilege reduction
- Sandboxing
- Virtualization
- …

- PATCH, PATCH, PATCH!
- Context dependent actions…

Endpoints…and perimeters



What about these… !?

Mobile devices

SOHO equipment

(Mesh) Wi-FI Access Points

Printers

Biometric/badge readers

Webcams

Access control systems

Powerline controllers

PLCs

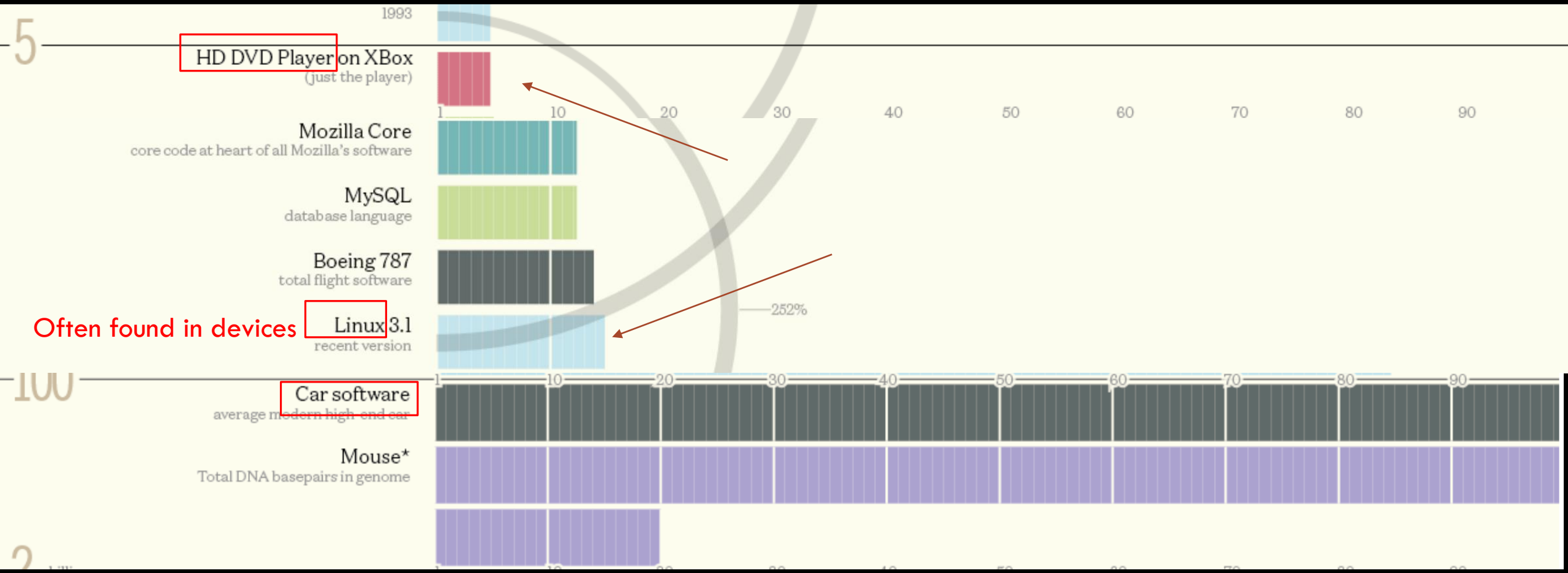
Sometimes labeled as …

"HARDWARE"

Source: *www.americasquarterly.org*

We call them devices.
And they are complex.

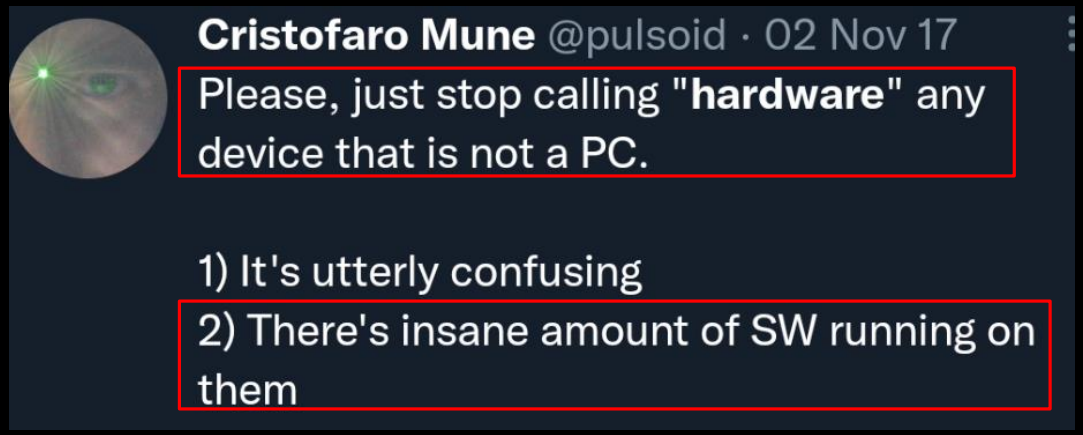
Devices have software…

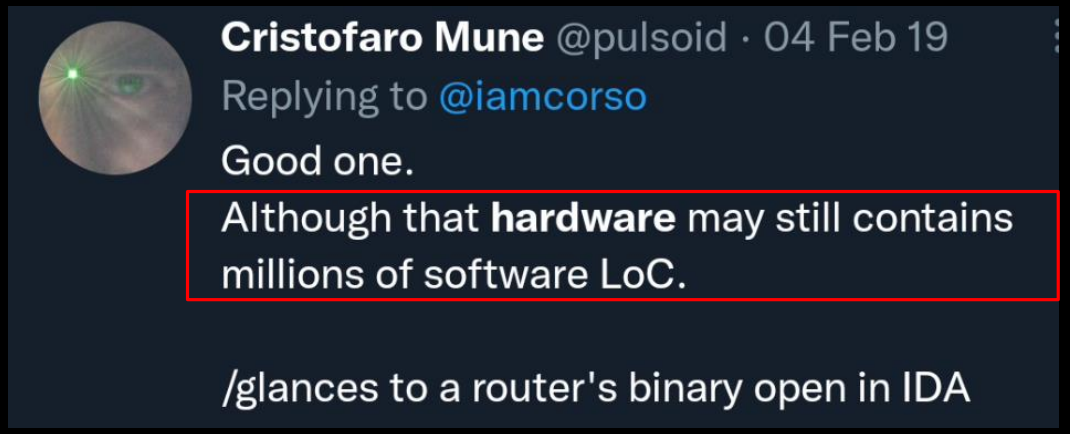


Source: www.visualcapitalist.com

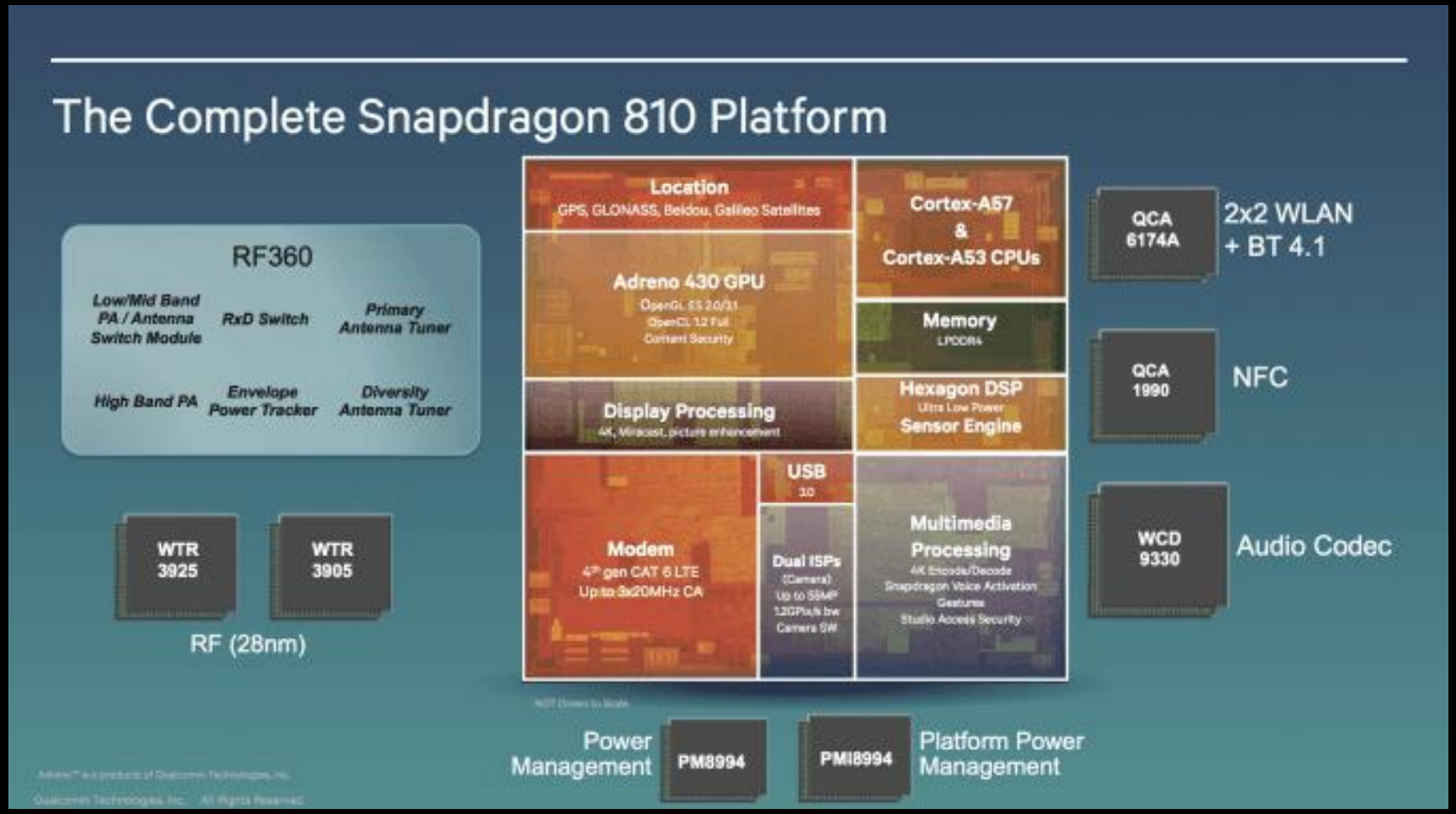
Well…


Cristofaro Mune @pulsoid · 10 Nov 15
We also need to stop calling **hardware** what is not **hardware**. twitter.com/blackswanburst...
Old bitshifter @blacksw... · 09 Nov 15
"We trust hardware implicitly and need to stop." - @securelyfitz


Cristofaro Mune @pulsoid · 02 Nov 17
Please, just stop calling "**hardware**" any device that is not a PC.
1) It's utterly confusing
2) There's insane amount of SW running on them


Cristofaro Mune @pulsoid · 04 Feb 19
Replying to @iamcorso
Good one.
Although that **hardware** may still contains millions of software LoC.
/glances to a router's binary open in IDA

Devices have powerful hardware…



Qualcomm Snapdragon 810 (2015)

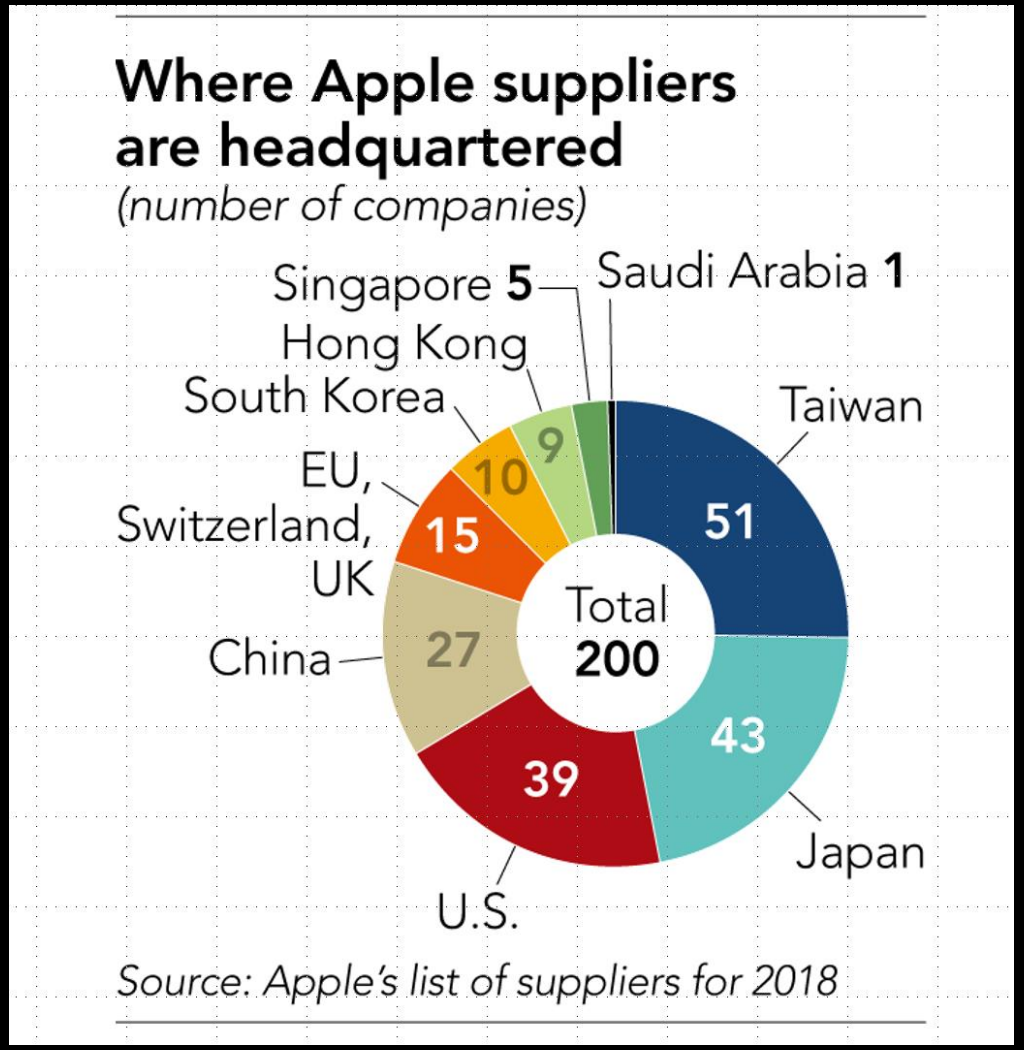
Who “owns” a device…

Actually…

Accelerometer
Bosch & Ivensense
Baseband Processor
Qualcomm
Batteries
Samsung & Shenzhen Desay Battery Technology
Chips
Cirus Logic, Samsung, TSMC, MicroSemi, Broadcom & NXP
DRAM
TSMC & SK Hynics
eCompass
Alps Electric

**from capitalistlad.wordpress.org*

Example: Apple suppliers 2018



Who owns a device?

“Nobody FULLY owns a device.”

How do we purchase them?

Generic

Price

Features

Security

In summary. Devices…

- Can rely on a large amount of software
- Can have powerful hardware
- Are the result of a wide ecosystem effort
- Are often purchased with little or no security criteria

What can go wrong?

Let’s find out…

Let's consider two scenarios

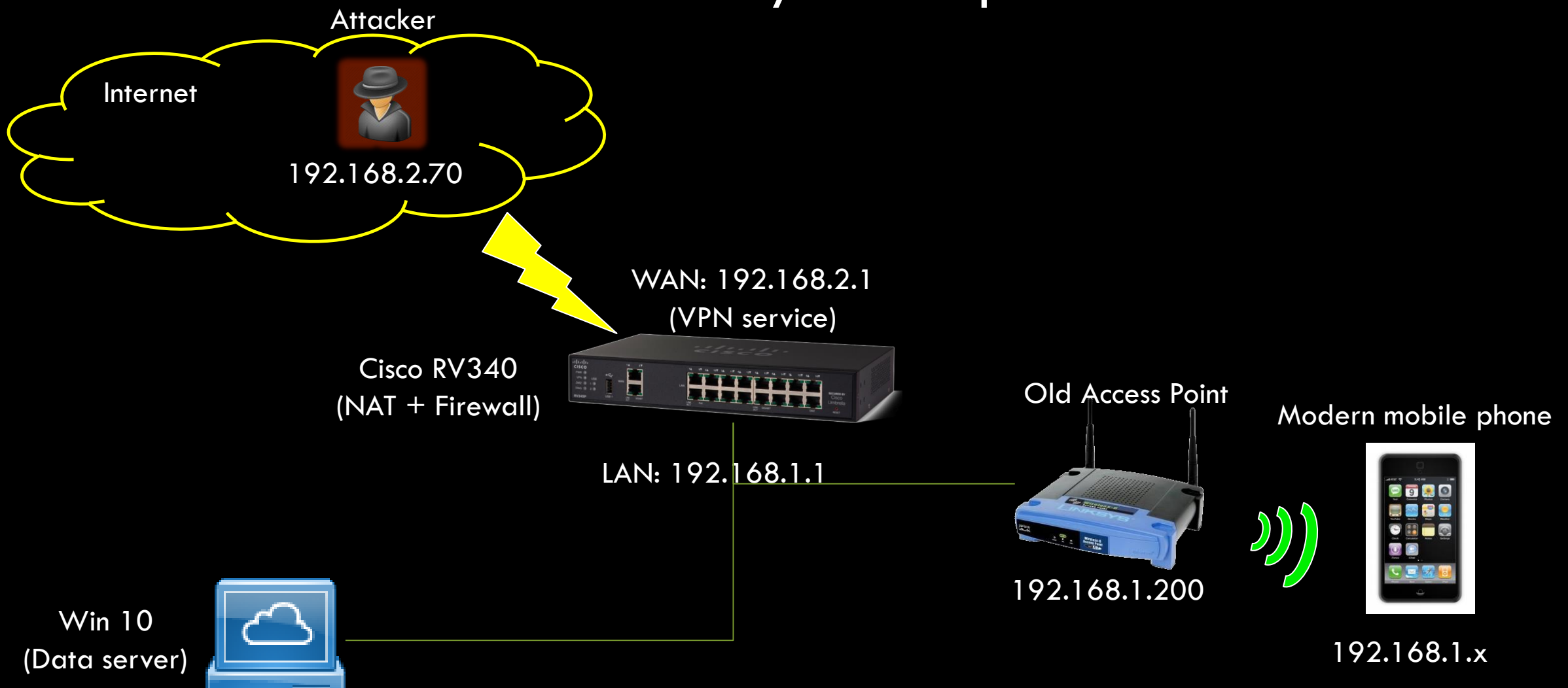
Corporate

Attacker aims to confidential data

Critical infrastructure

Attacker aims to infrastructure control

Our “toy” example



Our attacks

- Will be ALL device-based
- ALL using on public vulnerabilities
- Will encompass multiple stages

LIVE Demos!

Entering the front door.

Cisco RV340

- SOHO router from Cisco
- Target at PWN20WN 2021

- CPU: ARMv7 (→ 32 bit)
- Byte “sex”: Little Endian

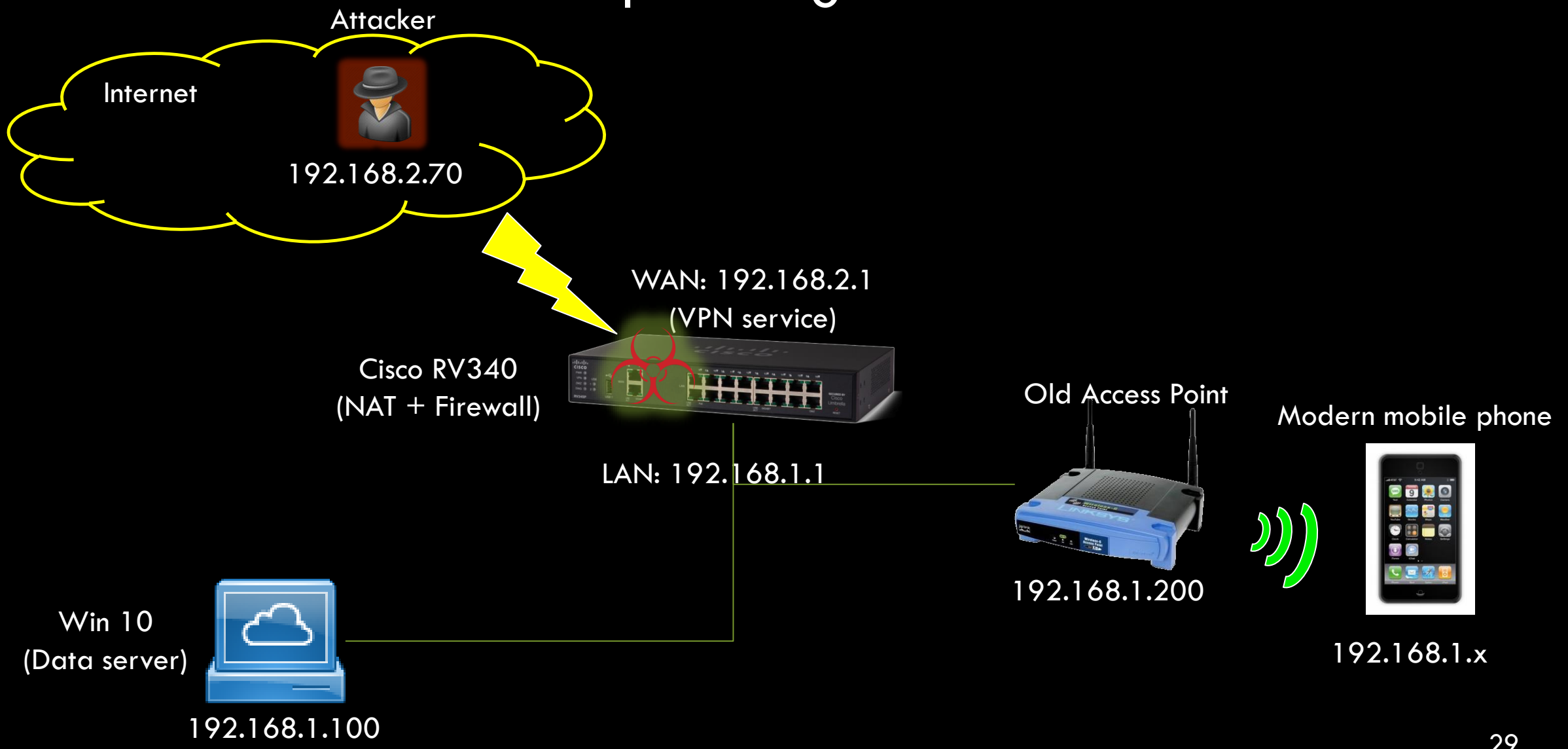
- Configured to provide VPN services over WAN (TCP 8443)

Our attack

- CVE ID: CVE-2022-20699
- Credits: Flashback Team at Pwn2Own
- Vulnerability in the SSL VPN server code
- Allows for RCE as root over the WAN interface.
- Patch released?: Yes. February 2, 2022
- Exploit code released and already present in Metasploit

Let's see it in action!

Comprimising from WAN



Demo.

Observations

- How would you detect such an attack?
  - VPN service is authorized → connections are legit
  - Service is encrypted
  - Usually no EDR agents…
- Any idea for mitigation?
- What about response?
  - Fix is available.

PATCH, PATCH, PATCH!

Actually… I have questions.

- Do you know:
  - how many devices are present in your organization?
  - Manufacturer, model and firmware versions?
- Do you follow device-related security bulletins (and research)?
- How do you know that you…

Have to patch?

Summary

- Devices may be a way into your infrastructure.
- It may be quite hard to detect a compromise
- Protecting devices require establishing processes
  - Similarly to what we have for other assets and endpoints.

Devices are endpoints too

Jumping over security boundaries.

Insecure devices

- …may always be present
  - Devices often selected for functionalities (i.e. it just works!)
- Their security status may easily go overlooked
  - Unless a process is in place.

- Scenario:
  - One old Access Point is used to temporarily extend coverage.

Linksys WAP54gv3

- Old but once common (~2010)
- Several vulnerabilities published:
  - Only one got CVE assigned
  - Fix availability? Unknown.

- CPU: MIPS @ 200 Mhz (Broadcom SoC BCM5352)
- Byte “sex”: Little Endian

- Very little memory (flash and DDR) and tooling on device

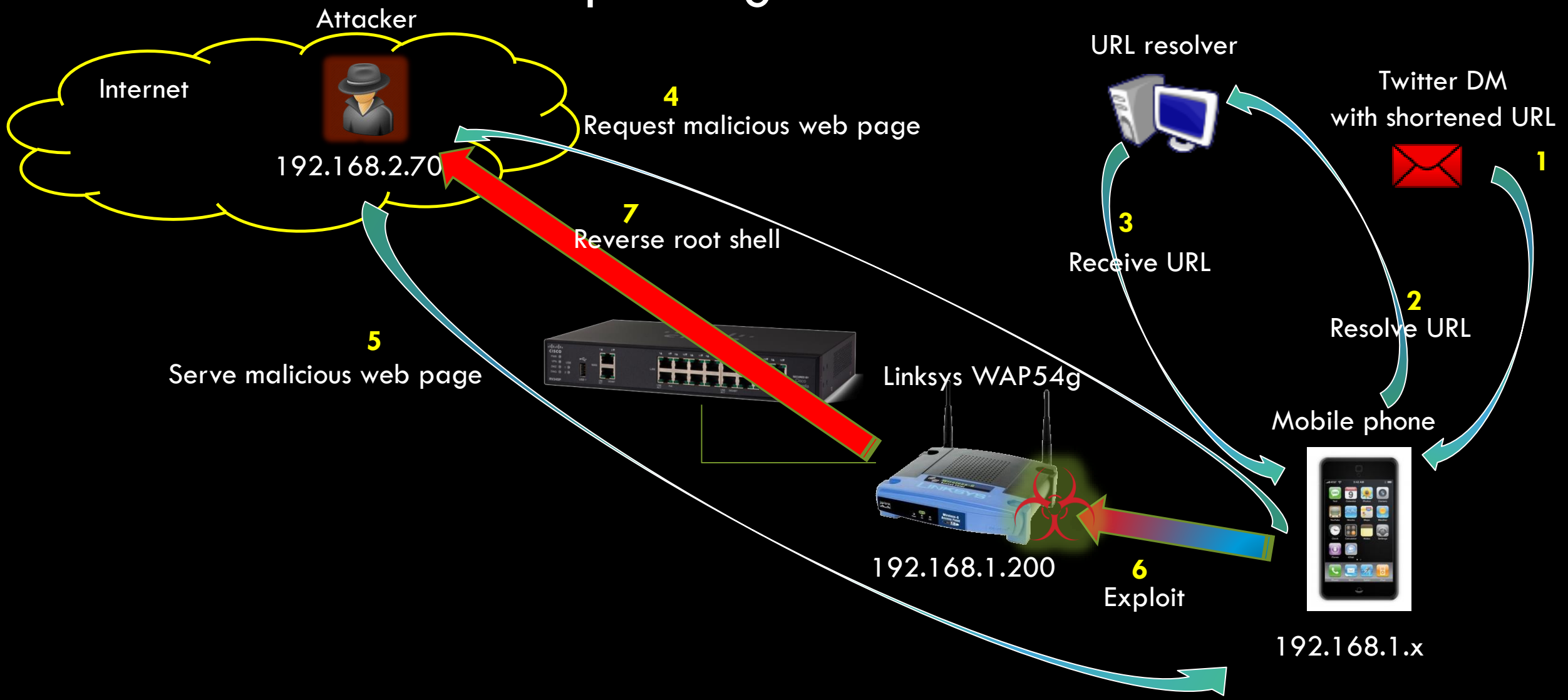
Vulnerability overview

- CVE ID: CVE-2010-1573 + No CVE assigned vuln (stack overflow)
- Credits: ☺

- Vulnerability in the HTTP server code. Allows for browser pivoting!
- RCE as root over the Ethernet interface.
- Interface not reachable from WAN, but…

We can bounce off a connected device!

Browser pivoting on Mobile Phone



Demo.

Observations

- How would you detect such an attack?
  - All pages can be served over HTTPs
  - Mobile → AP connection not monitored

- Mitigation: Why is an Access Point allowed to freely access the Internet?
  - Network segregation and firewall policies

- Response?

PATCH, PATCH, PA…

Sorry…

- No fix available.
- Device is End-of-Life (EoL)
- The device will be vulnerable forever

- Only response possible is…

Throw it away!

End-of-Life (EoL)

- EoL condition pose serious threats:
  - Security vulnerabilities cannot be resolved
- Often planned ahead in IT security
  - Devices: ???
- `Particularly relevant for Critical Infrastructures
  - Expected lifetime may reach 30 years.
  - Can you patch in 10 years after purchase?

Also an Ecosystem threat

- Attackers are actually using EoL devices
  - Example: see our research here on DSL-2640-B
- 14k+ DSL-2640B reachable over the Internet, AFTER 6 years EOL
  - Shodan only reported2
- EoL → Exploits with a guaranteed infinite lifetime
- Actively exploited and part of a botnet
  - Aggregated upstream bandwidth: ~49Gbps:

Prevention?

- Possible at procurement phase
- Ask questions on security support:
  - Duration of technical and security support
  - Communication of vulnerabilities/Security Advisories
  - Average time to patch
  - Internal security team
- Make it part of your Vendor Selection process → Will create market pressure

You are purchasing security. (Not only a device)

Do you protect FROM devices?

Lateral movements between devices.

Cisco RV340: LAN side vulns

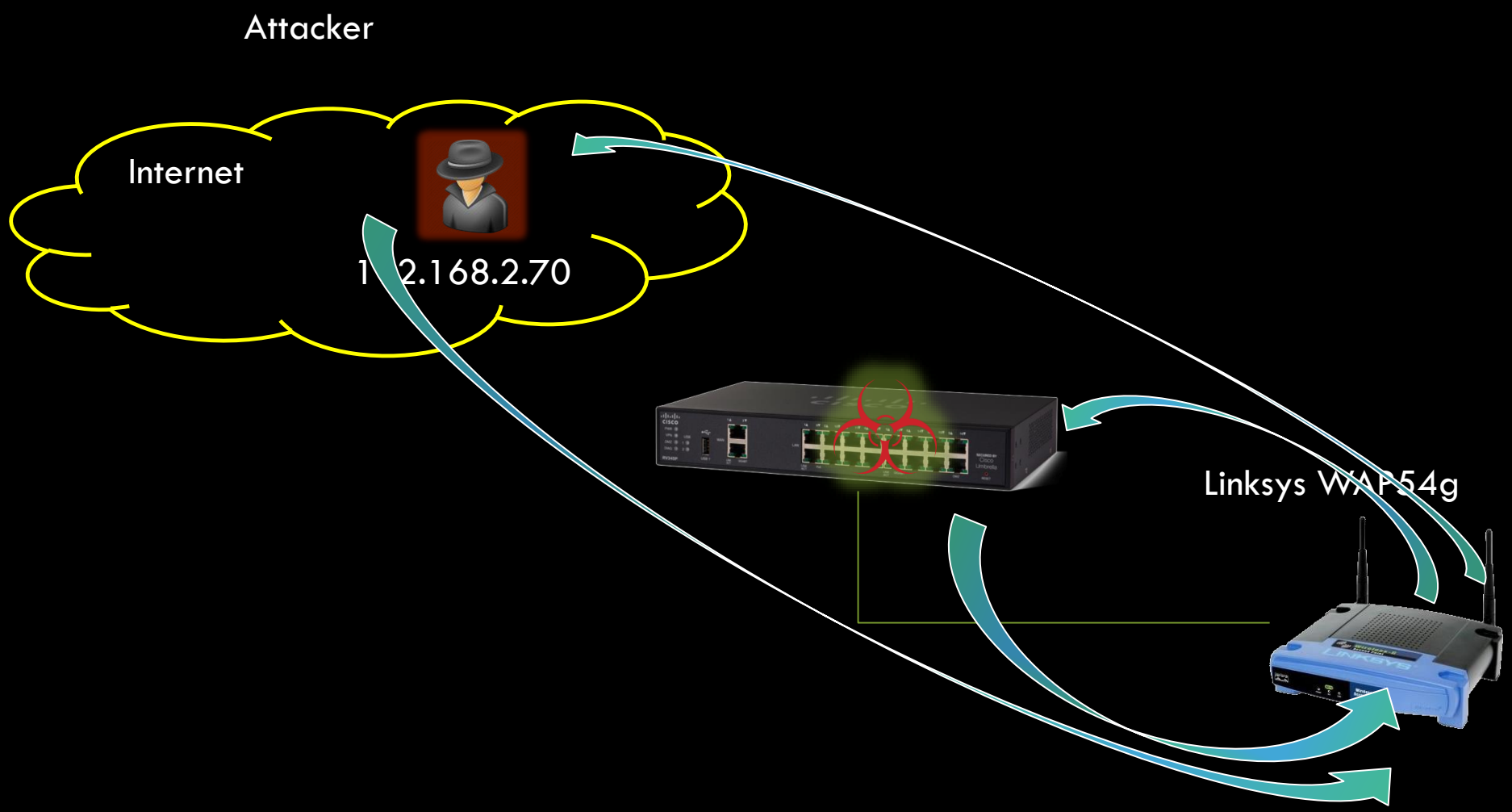
- Still from PWN20WN 2021
- CVE-2022-20705, CVE-2022-20707:
  - HTTP server auth bypass + command injection
- CVE-2022-20708:
  - Command injection as root (for authenticated users)

Attack plan

- Lateral movement between Access Point and router:
  - We attack Router LAN interface…from the WAP54G!
- We set the Access Point as a pivot:
  - Push tooling, establish tunnels,…
- We can now interact with the LAN interface directly
- Chain 3 vulnerabilities:
  - CVE-2022-20705 and CVE-2022-20707:
    - Execute command as unprivileged user ('www-data')
    - Inject a fake admin session token
  - CVE-2022-20708 to run command as root

Let's see it in action!

Pivoting on a compromised device



Demo.

Prevention?

- Possible at procurement phase
- Ask questions on product security:
  - security certification
  - regular security testing
  - security code reviews
  - Secure SDLC practices
  - …
- Make it part of your Vendor Selection process → Will create market pressure

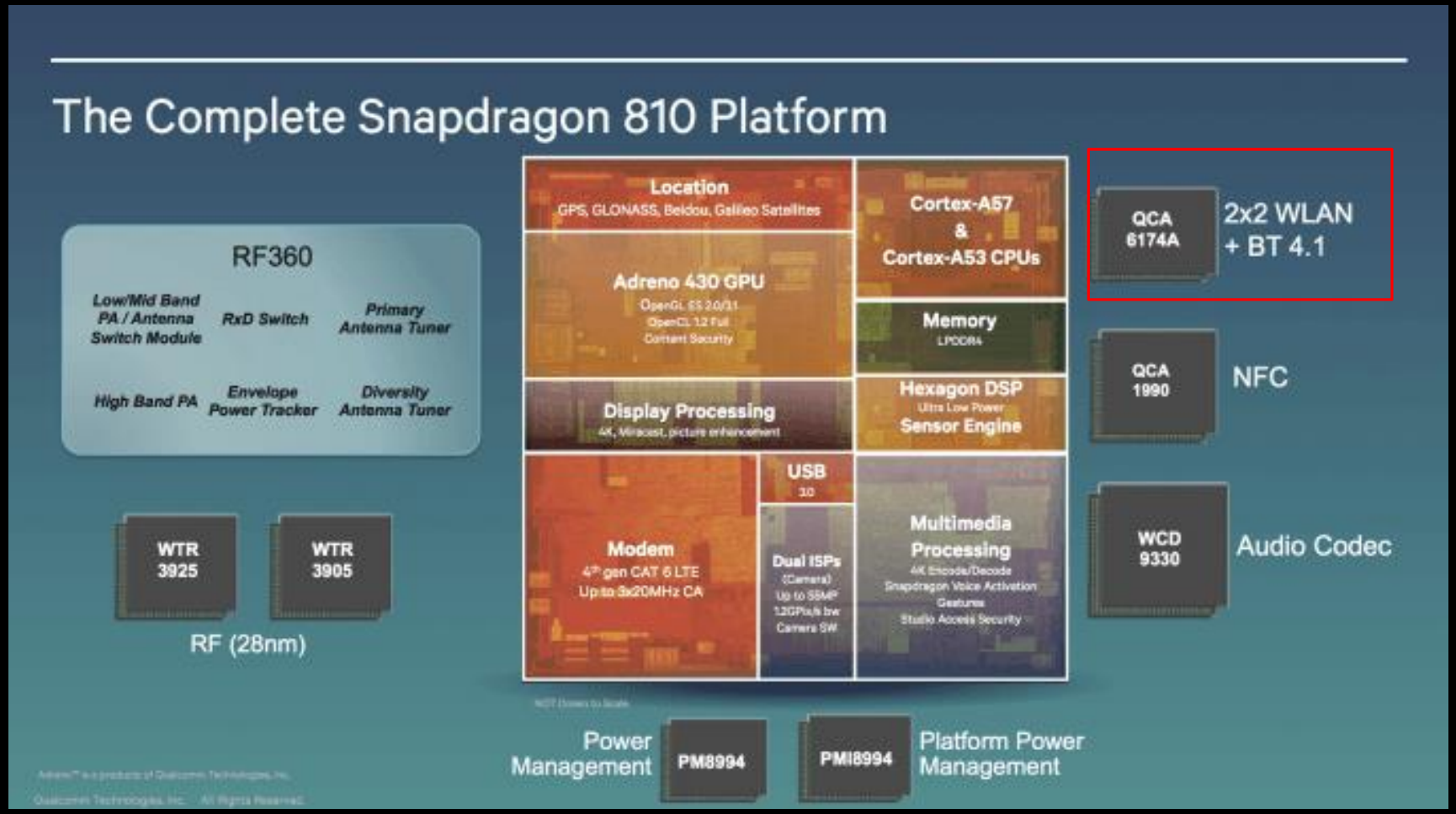
You are purchasing security. (Not only a device)

Radio interfaces.

Modern devices architecture

- Have fast and complex radio communications:
  - LTE, 5G, WiFi, Bluetooth…
- Need for rich, yet responsive devices
- Most code typically run on Application SoC
  - User application, Kernel, Hypervisor,…TEE
- Protocol handling often off-loaded to separate System-on-Chips (SoCs):
  - Baseband, WiFi + BT,…

Example: Snapdragon 810



Again…not “hardware”

- Wi-Fi SoCs often handle the full stack of radio communications
  - FullMAC WiFi implementations: PHY, MAC, MLME
- Complex firmware code implements WiFi standards
- Data packets directly passed to kernel (on Application SoC):
  - E.g. via DMA functionalities provided by PCIe

Broadpwn (2017).

Wireless Multimedia Extensions (WMM)

- Extensions to the 802.11 standard
  - Allow for traffic prioritization (QoS)

- During association clients and AP exchange Information Elements (IEs) on WMM support

- This happens before any association is established:
  - i.e. no password is needed

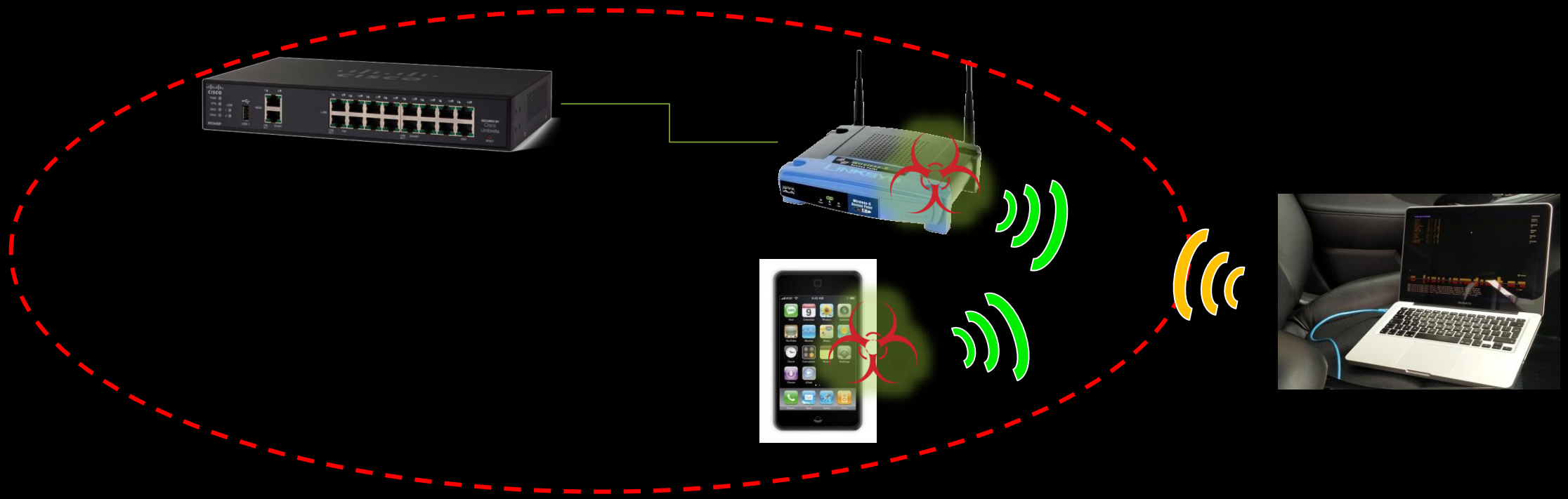
The vulnerability

- Buffer overflow in parsing IEs.
- Identified by Nitay Artenstein (Exodus Intelligence)
- Applicable to the entire family of Broadcom BCM43xx Wi-Fi SoCs
- Millions of devices impacted
  - Mostly mobile phones, but not only.
  - HTC, LG, Nexus , full range of Samsung flagship devices…

The exploit

- Arbitrary code execution on the WiFi SoC.
- No exploit mitigations:
  - Entire memory is RWX
- Failed exploit easily unnoticed by a victim
  - e.g. WiFi icon disappears
- No user interaction required
- Techniques may also allow to compromise Application SoC

What's the impact?



Proximal attackers may compromise devices inside the perimeter

Observations

- WiFi coverage is everywhere
- Detection?
  - No IP traffic
  - Attacker can be at convenient distance
  - Hard to see side effects
- Perimeter becomes irrelevant
  - Border security ineffective
  - May target devices in very sensitive networks

Can it get any worse?

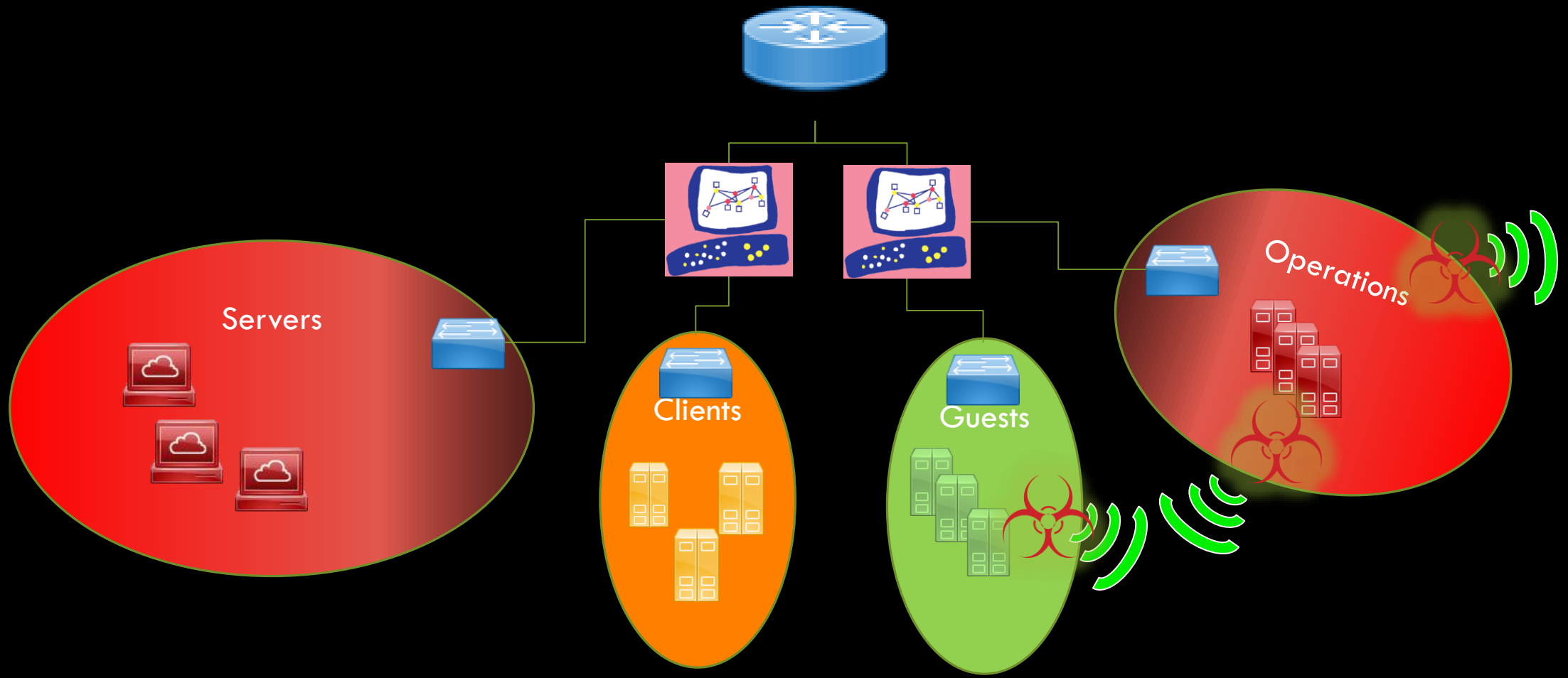
- Yes. When the vulnerability is "wormable"
  - Payload running in the WiFi SoC may compromise a nearby device!
  - No need to compromise the Application SoC

- WiFi coverage often provides overlapping signals
  - i.e. an AP may listen (and exploit) another IP in range

- An attacker may compromise the entire WiFi infrastructure…

…without generating any IP traffic at all

Accessing critical networks



Conclusions.

We have seen that…

- Devices can play a significant role in infrastructure security
- You need to protect devices as well as FROM devices
- They may yield hard to detect attacks
  - Lateral movements between devices
  - Attacks leveraging radio protocols
- Perimeter security can be completely jeopardized
- Usual IT security practices may be ineffective
- No actual control on the security of devices:
  - Usually not a priority

What can we do?

- Establish processes
  - Know your security exposure (e.g. keep an inventory)
  - Be aware and informed
- Make sure to buy security (an not only a device)
- ASK for security:
  - Support, patches, fixes, bulletin
  - Assess the quality of the product AND the Vendor
- Perform security testing for critical uses
- Involve experts knowledgeable in device security

ræ lize

Thank you!

Cristofaro Mune
cristofaro@raelize.com
@pulsoid