merlin cyber

Layer 1 Network Security

Dealing with Stealth in Cybersecurity

Dean Webb

Cybersecurity Solution Architect

What do you see here?

There are spheres and boxes and arrows and clouds and shields and gears and people...

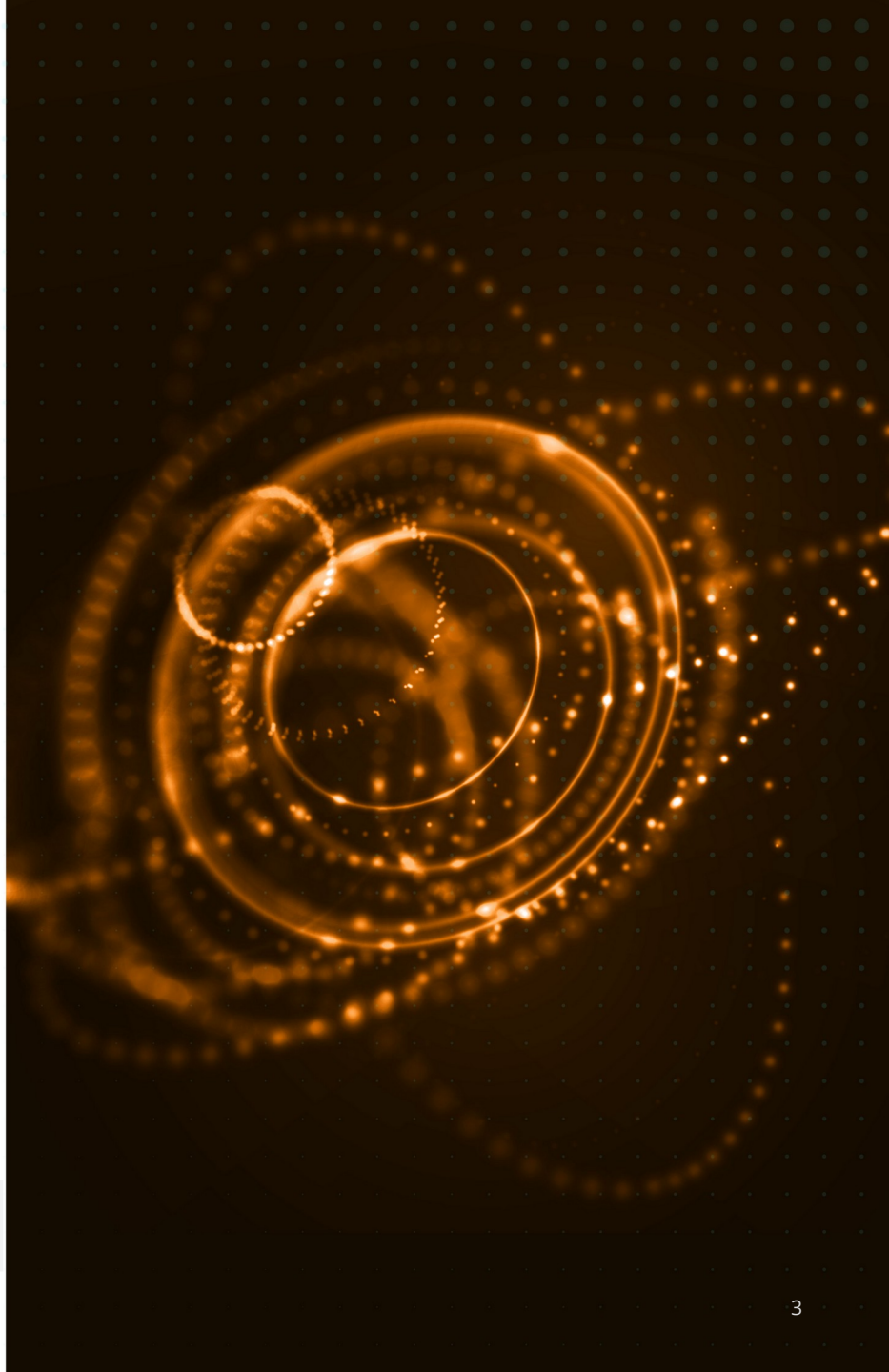
But did you also see the lines between the images?

THE ATTACKERS DO.

Physical Layer

The Sneakiest Attack Vector

- We have 7 layers in the OSI model.
- 6 of those layers have commonly-used cybersecurity tools. We understand attack vectors in those layers.
- The ***physical*** layer, however, is largely ignored.
- Attackers with access to the supply chain are making physical layer moves – not a Malware aaS use case!
- We need a security tool to protect us from this “invisible” attack vector.



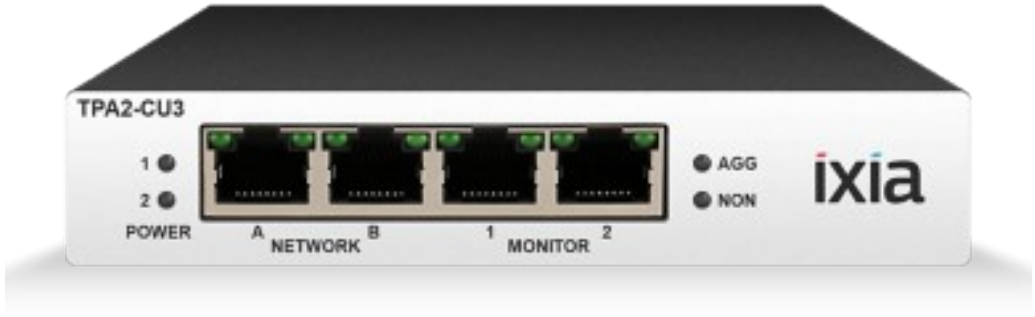
Layer One Threats

No IP address, no MAC address: how do they work?

Network Taps

- Inexpensive, only a few hundred $
- No power supply needed, thanks to PoE
- High speed options available: optical taps at 40Gbps
- Reads everything on the wire and outputs to monitor
- No traffic addressed to it directly, so no IP or MAC address needed: it Just. Reads. Everything.

Use Case: Visibility



Passive TAP devices connected to secured network running privileged customer data; MAC-less devices invisible to all other tools.

Scanning tools will not see these devices, as there is no layer 2+ information to be scanned on them.

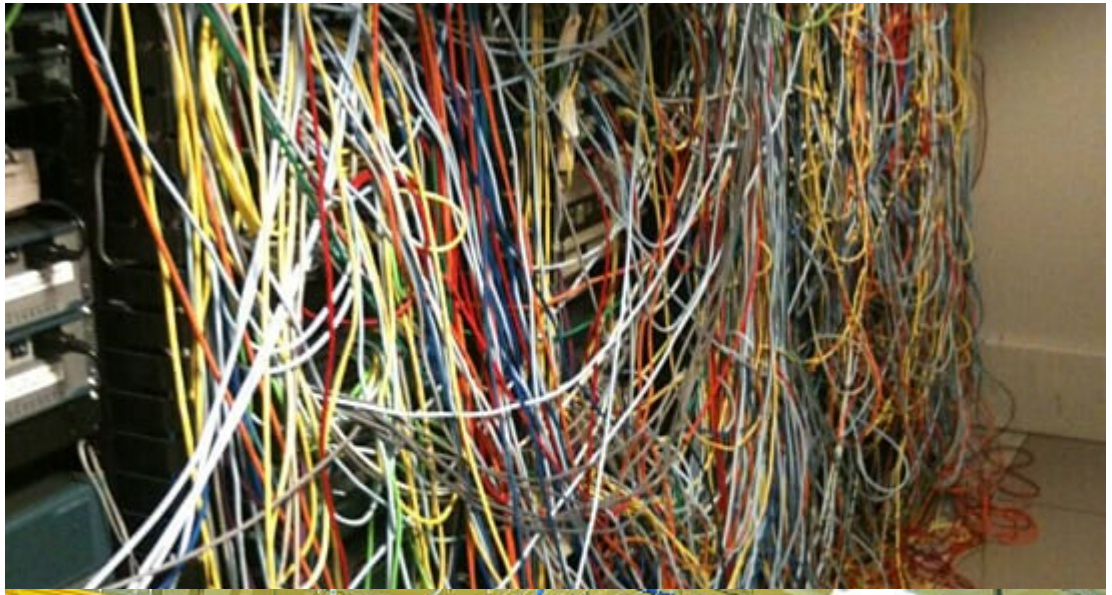
A Word About Datacenters…

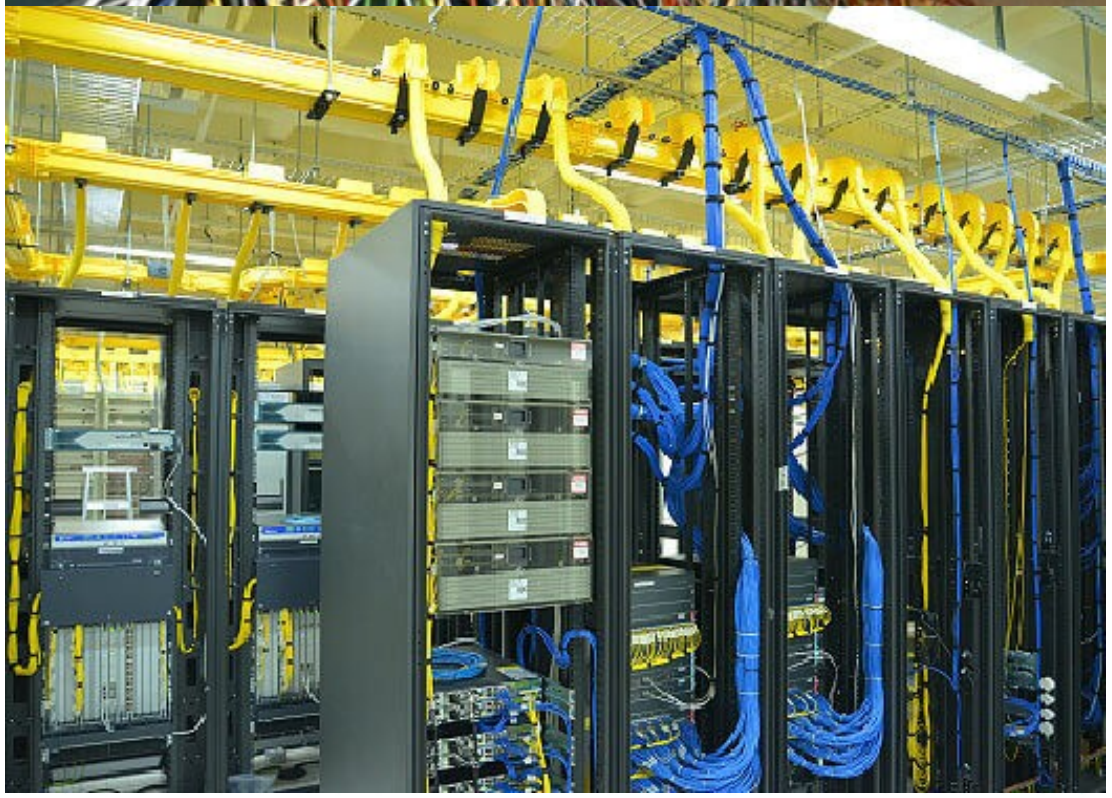
"We have met the enemy and they is us!" – Pogo Possum

Datacenter Obstacles to Security

- Touching anything = change control hell
- If something is neat and tidy, we don't ask questions
- If something has stern post-it notes, we give it wide berth
- Mess or perfect, no way to follow cables
- We ***think*** we can trust everyone signing in and out
- "Don't touch the DC!" – many orgs have this roadblock

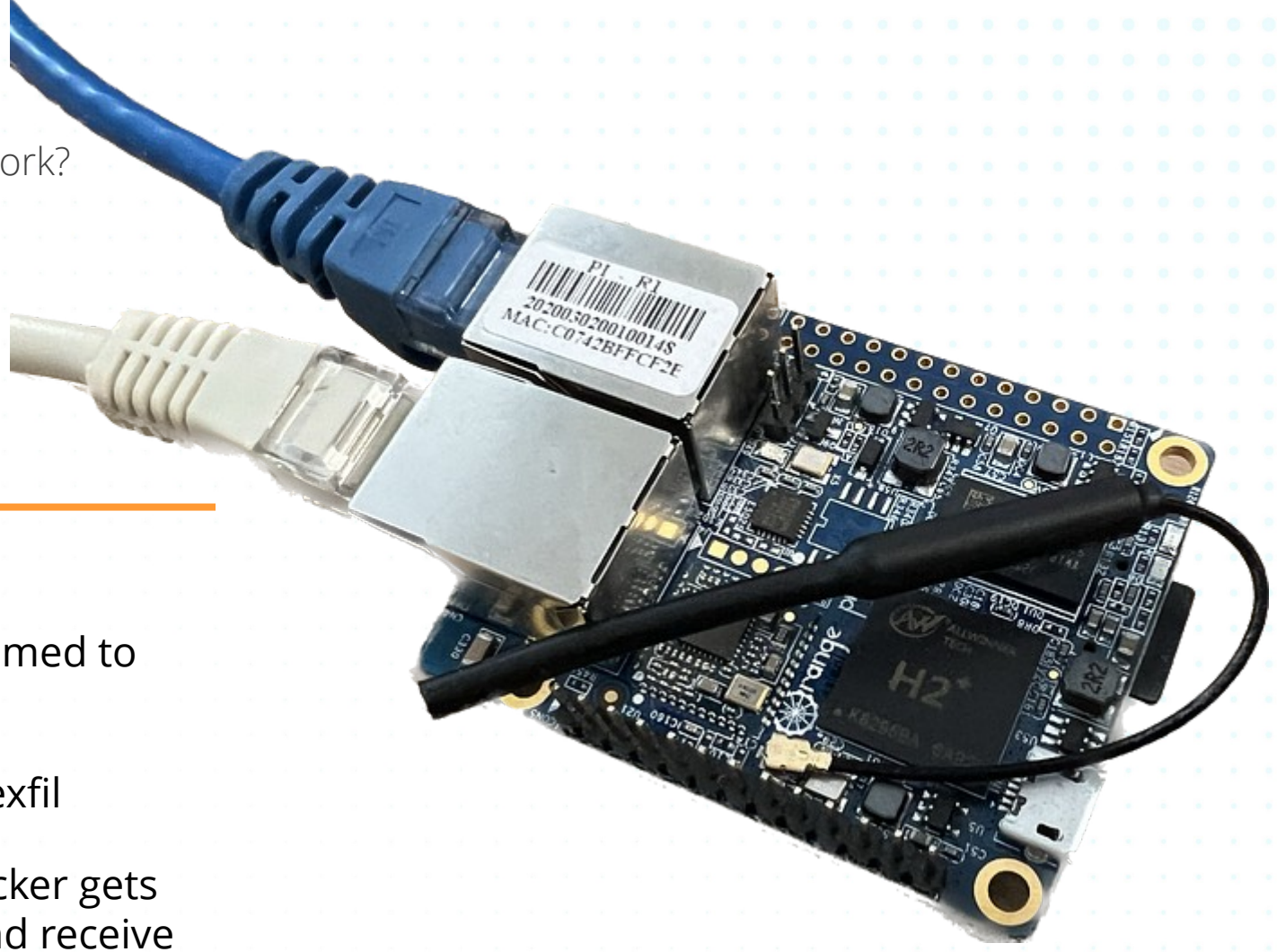
Once in, a datacenter threat will be nearly impossible to visually detect and remove. If it is also avoiding detection at layer 2 and above, it's game over for the defenders.





Layer One Threats

No IP address, no MAC address: how do they work?



MAC-less Micro PCs

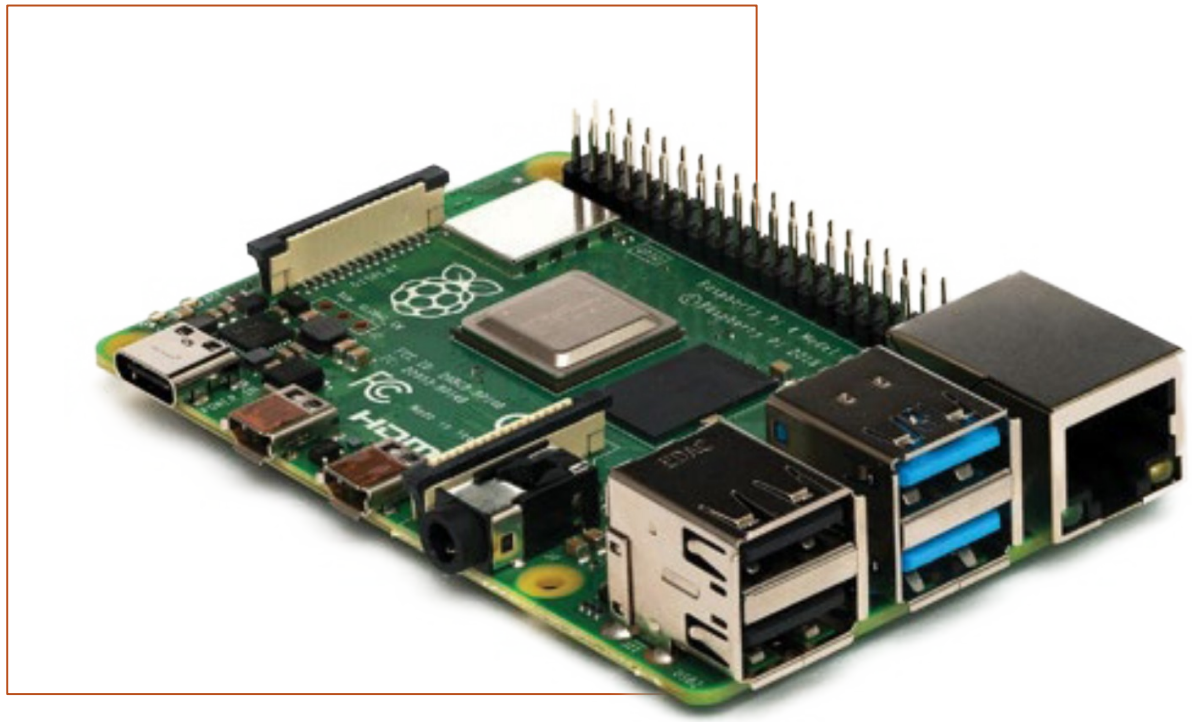
- Bridges between the Ethernet cables
- Ignore the MAC on the sticker, can be programmed to have no MAC address
- Check out the wifi antenna, nice for that data exfil
- Legitimate device 802.1X auth means this attacker gets to “ride along” with that legit auth, can send and receive with legit IP/MAC
- Can be programmed to forward along data to/from downline device, so it never “knows”
- Imagine this inside an official-looking box, in the racks…

Use Case: Insider Threat

Tier 1 Bank Leaking Data; Attackers used Transparent Network Devices. Running out-of-band, undetected for months. They were inline with server assets that passed 802.1X auth.

In 2019 a US Federal Agency facility had been **hacked by a Raspberry Pi device** that was linked to the agency's network without authorization. It used a MAC address that allowed it to bypass 802.1X, claiming to be a normal IoT device.

Use Case: Insider Threat, Part Two



MAC Bypass List: makes it very easy for non-802.1X compliant devices, including attackers, to get on the network.

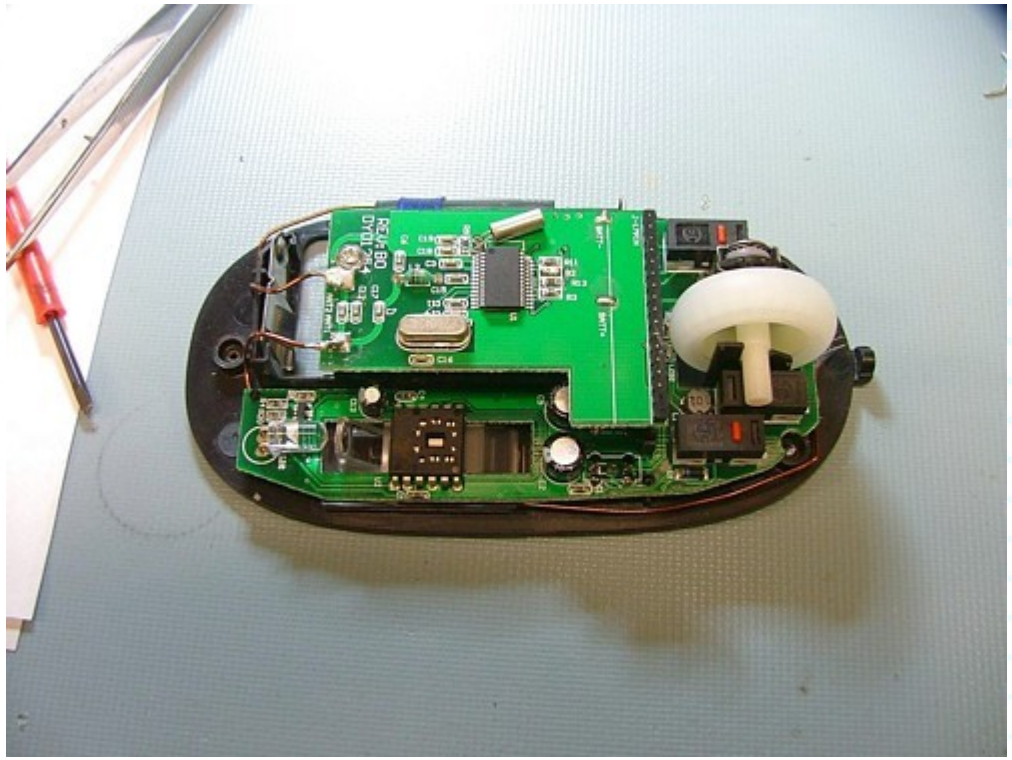
Bypass lists are built with the 6-digit vendor prefix on every MAC address, the Organizationally Unique Identifier (OUI). Program a device to have a MAC address with that OUI and a random set of 6 digits to finish it off, chances are it'll get on the network without a problem... or second glance...

Layer One Threats

No IP address, no MAC address: how do they work?

Physically Modified Hardware

- PLENTY of room inside the form factors of mice, keyboards, printers, door badge readers, and so on…
- Peripherals for targeting particular PC’s mouse clicks and typing: other devices for harvesting data sent to/from those devices
- Attackers not random: specifically targeting shipments to facility, may have someone on inside to make exact placements
- Devices are passive, will only capture data



Use Case: Supply Chain

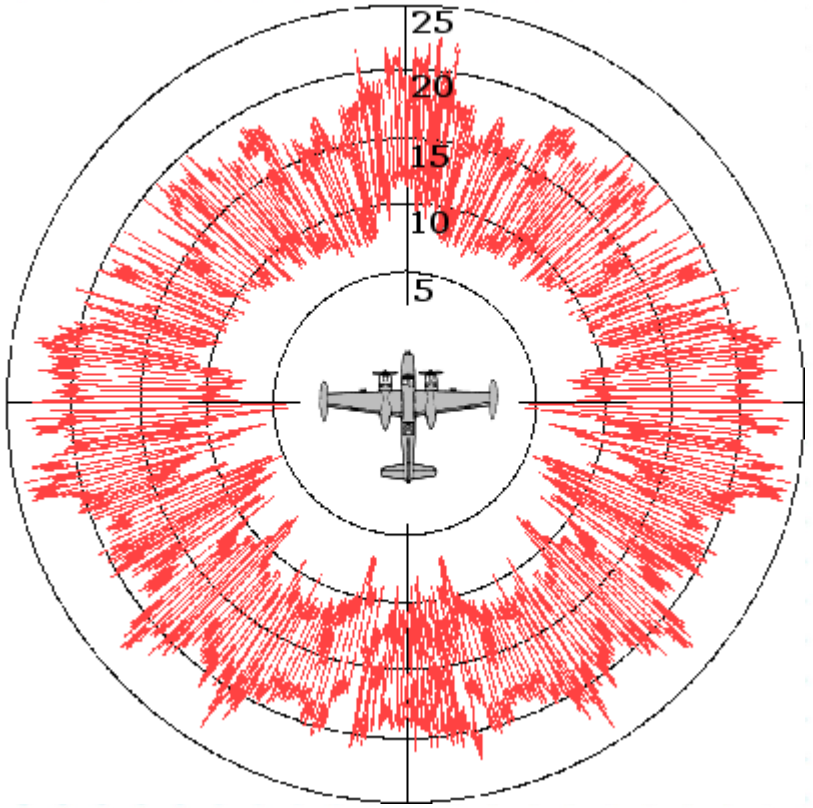
Attackers penetrated into air-gapped network **using a malicious peripheral device**; EDR/DLP reported a legitimate device.

Signatures – How We Detect Things

Some things you just can't hide…

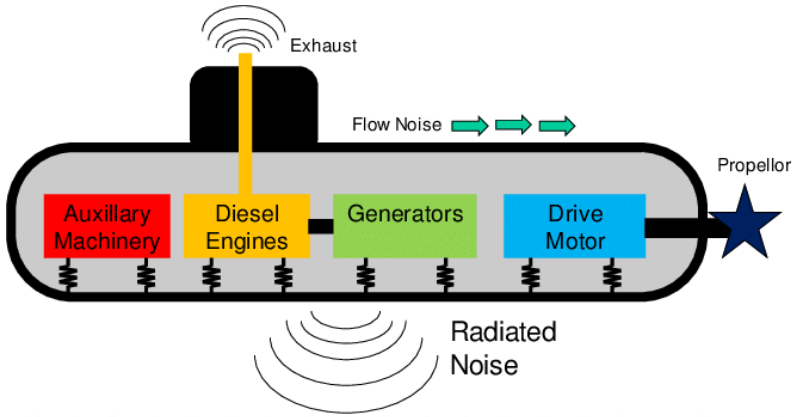
Radar Cross Section (RCS)

Detect aerial objects and determine what they are



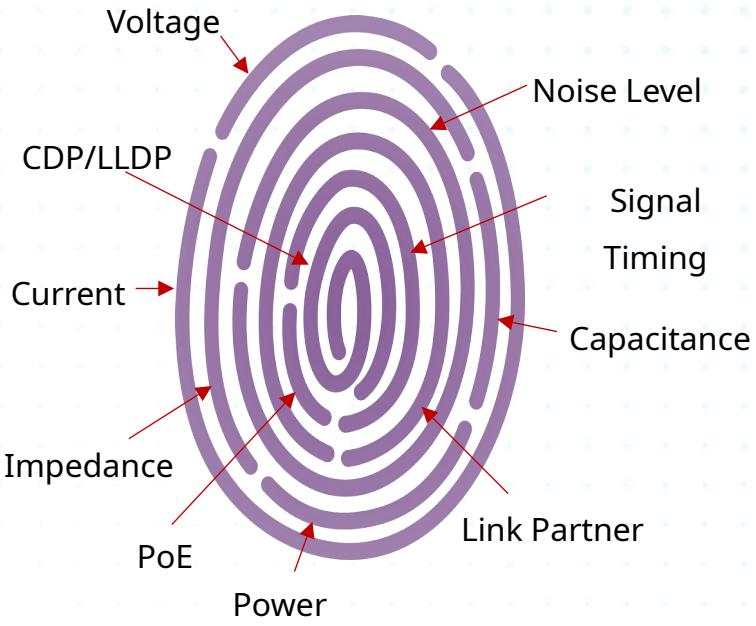
Acoustic Signature

There's USN quiet and then there's battery quiet…

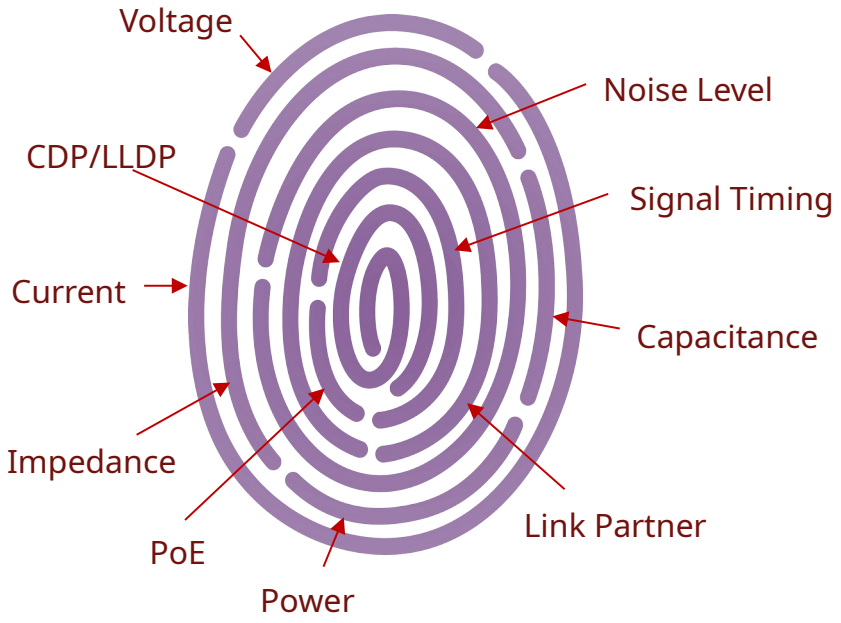


Hardware Fingerprint

Every device has one – changes will have new fingerprints



Hardware Fingerprints

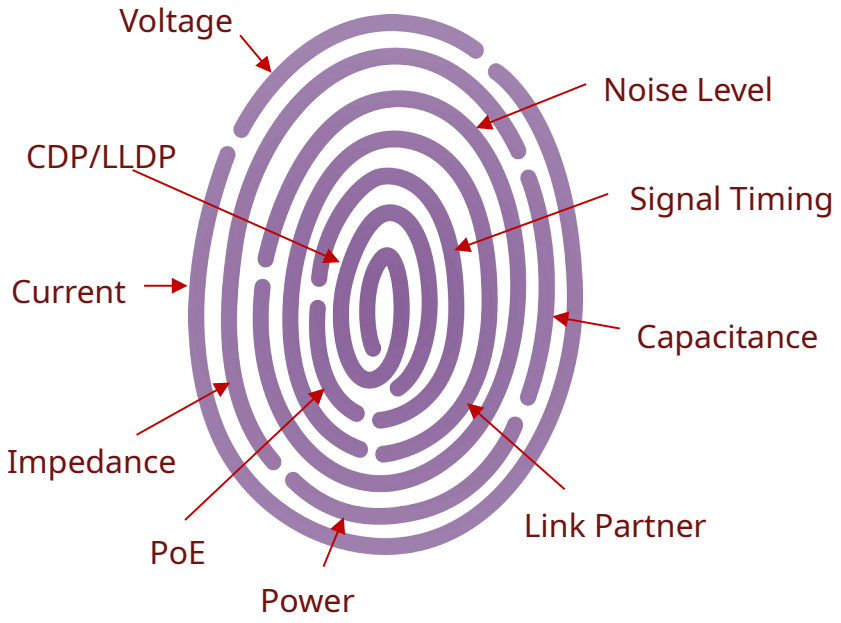


- Collecting Layer-1 data from existing Hardware
  - Modern network devices track power usage information
  - OS agent can track physical information on peripherals
- Generating Fingerprints based on multiple parameters
- Grouping devices based on IDs and Fingerprints
- Assessing risk based on unmatched Fingerprints
- Discovering new threats by using Bigdata and ML

Discovering devices based on physical fingerprinting will find what can’t be faked.

No traffic monitoring. Fast. Lightweight. Accurate.

Hardware Fingerprints



- "Fingerprint" match based on points of similarity
- Rating is given with a % confidence – more points, more confidence
- No similarity = device masquerading
- Similarity with key differences = device inline, along for the ride
- Devices degrading over time can be tracked algorithmically, will not generate false positives
- Manufacturing variability tracked similarly – "Law of Large Numbers" helps us in this case, with big datasets giving us expected ranges of variability.

Slight differences = manufacture variability or degrading over time
Large differences = something *different* is in play, investigate!

One More Use Case: Re-labeled Gear

The physical box, purchase order, MAC address and initial console logon all look like the device has no NDAA Section 889 issues. But the hardware fingerprint says otherwise…

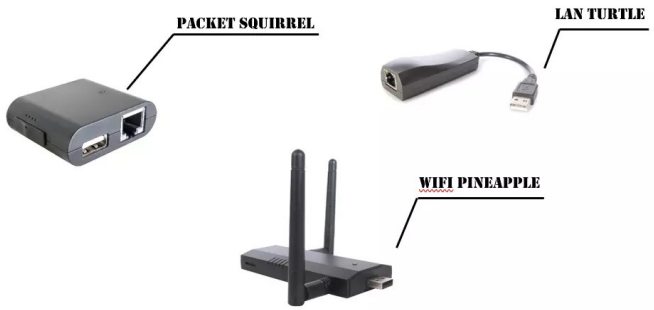
This is a real issue when a Section 889-prohibited firm has an associate firm acquire a non-prohibited manufacturer and then utilize parts from the Section 889-prohibited firm.

Resolving the Use Cases

Hardware Fingerprinting for the Win...

Network Taps

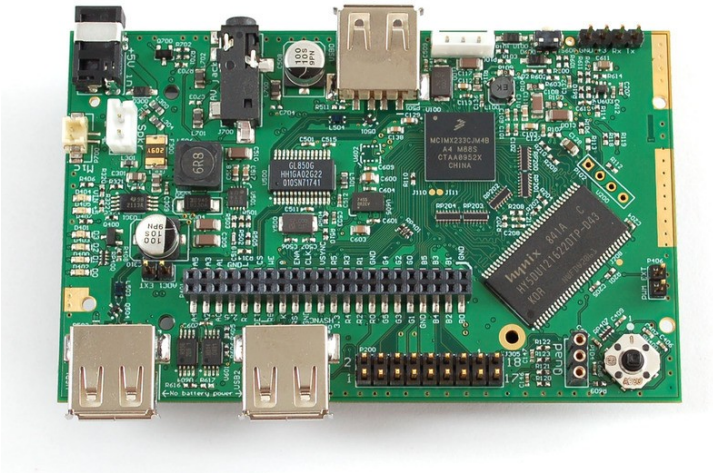
HF = HF for device PLUS *something else...*



Something else could be one of these things, which are not like the others...

Device Masquerading

HF seen != HF for device type



This is not a desktop phone, even though the OUI says it is.

Modified Hardware

HF = a known HF... for something that this *isn't!*

Through most of 2022, ADI was secretly relabeling Dahua gear.

DISCLAIMER: MERLIN IS A PARTNER WITH SEPIO

Merlin Partner

- **A leader in the Rogue Device Mitigation (RDM) market.**
- **Protects organizations from hardware-based attacks and threats.** Sepio Systems provides security teams with full visibility into their hardware assets and their behavior in real-time.
- **Sepio Network Security** provides full visibility into the network based on hardware fingerprinting and machine learning algorithms with the ability to detect any logically invisible attack tool.
- **Sepio plays nicely in the datacenter,** by the way...

merlin

Merlin is the premier Public Sector growth acceleration platform for cybersecurity companies seeking to rapidly scale their businesses within the U.S. Federal and State, Local and Education (SLED) markets. Merlin's one-of-a-kind business model leverages innovative technologies, trusted relationships, and capital to develop and deliver groundbreaking security solutions that help Public Sector agencies minimize risk and simplify IT operations. Merlin selectively represents prominent cybersecurity brands and invests in visionary, emerging technologies. By bringing select partners and portfolio companies together into Merlin Labs, cybersecurity engineers integrate, test, and deliver more holistic security solutions that are entrusted to solve the Public Sector's most complex cybersecurity challenges. This approach helps the U.S. Public Sector save time, money, and other resources while more effectively securing its systems, data, and users no matter how requirements evolve.