RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HTA-R02

Air Gap Hopping with Musical Fans: Proving a False Sense of Security

Aaron Rosenmund

Head of Research and Content Development – Security
Pluralsight
@arosenmund

Overview

- Introduction
- Setting the Scene
- Basic Side Channels
- Advanced Side Channels
- Chain of Compromise
- POC Demo
- Advanced detections for advanced attacks

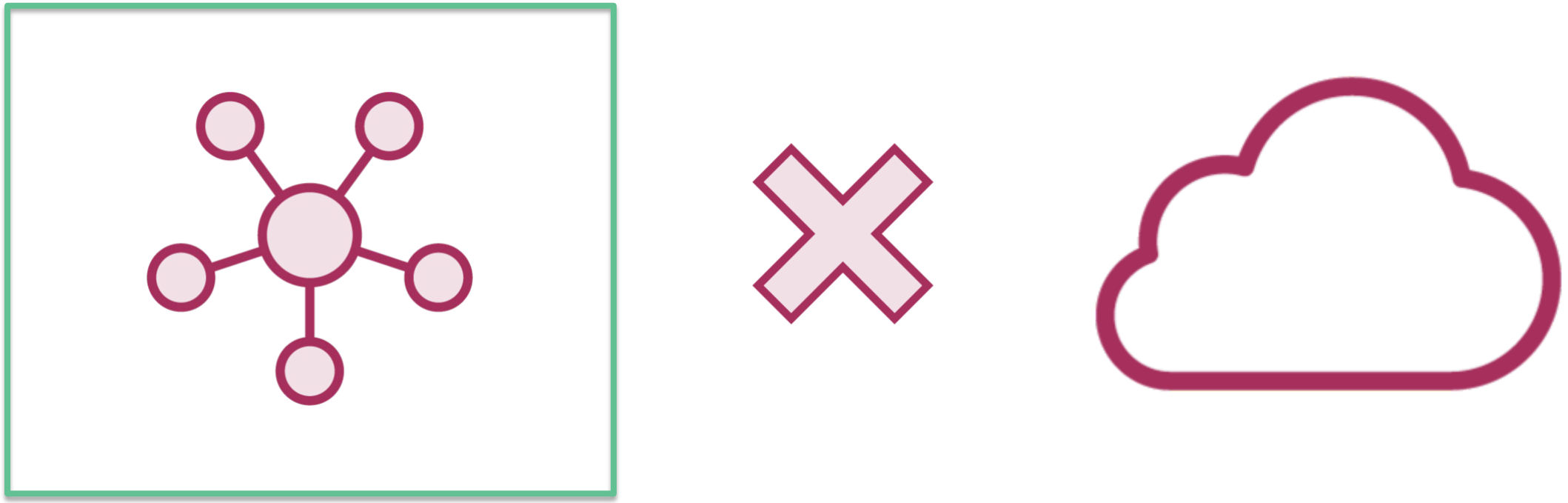
RSAConference2020

Introduction

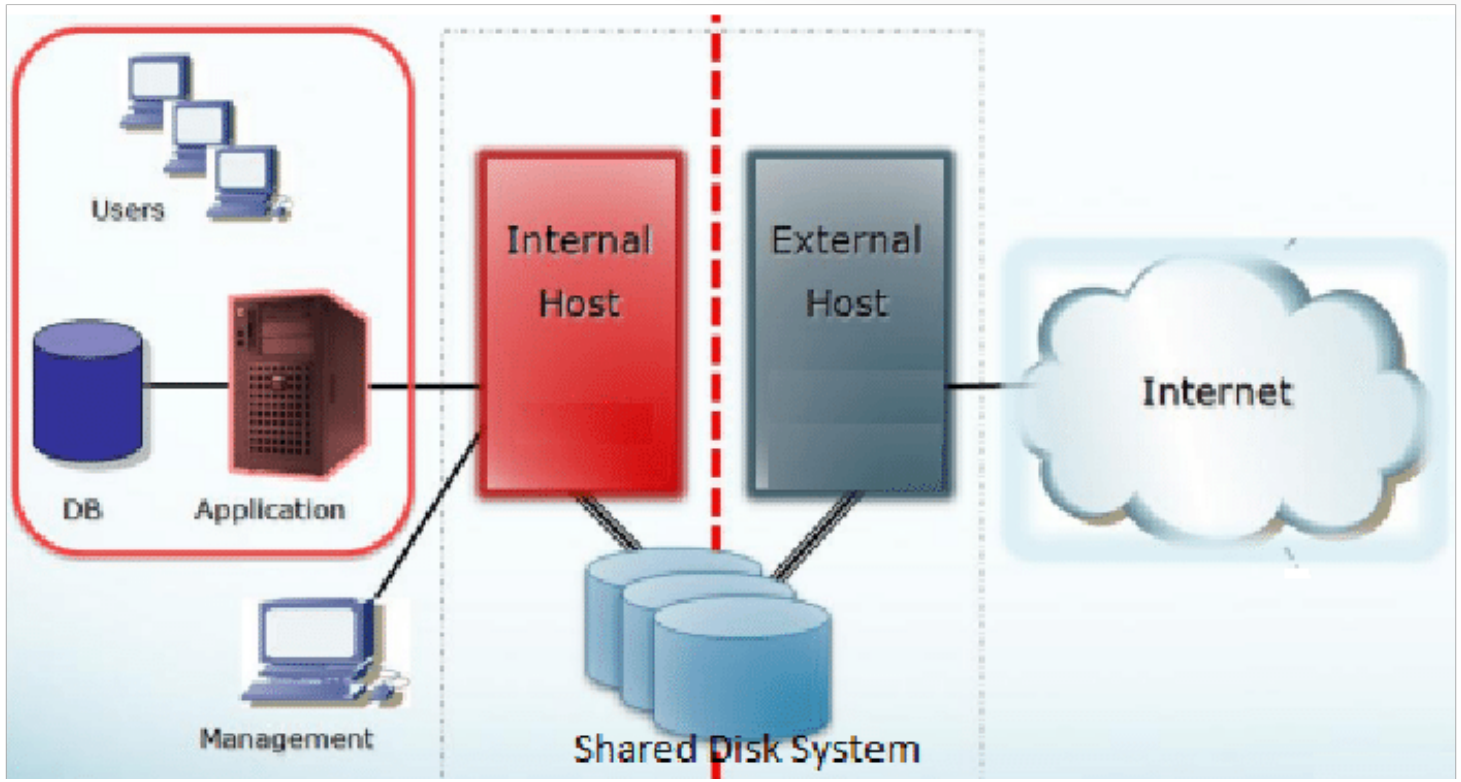
Defining the Problem

What an Air Gapped Is

Air Gapped Network not connected through conventional wi-fi or wires (fiber or ethernet) to the internet.



Rare that networks are fully air gapped

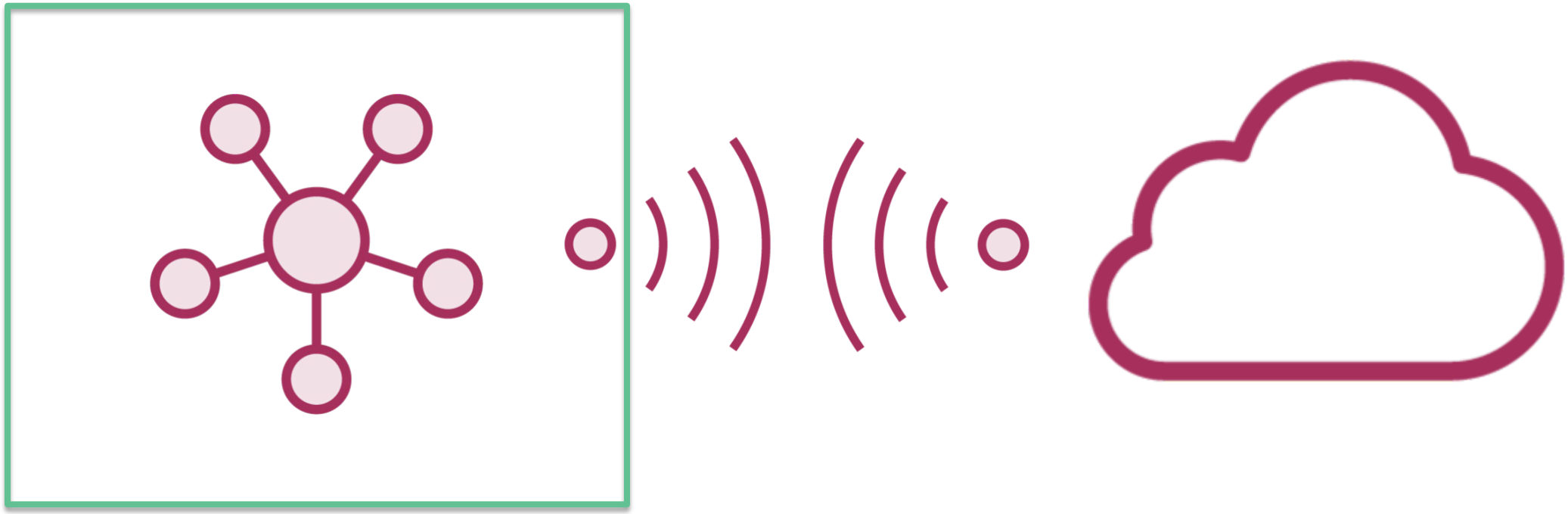


ANY SHARED RESOURCES BREAK THE AIR GAP

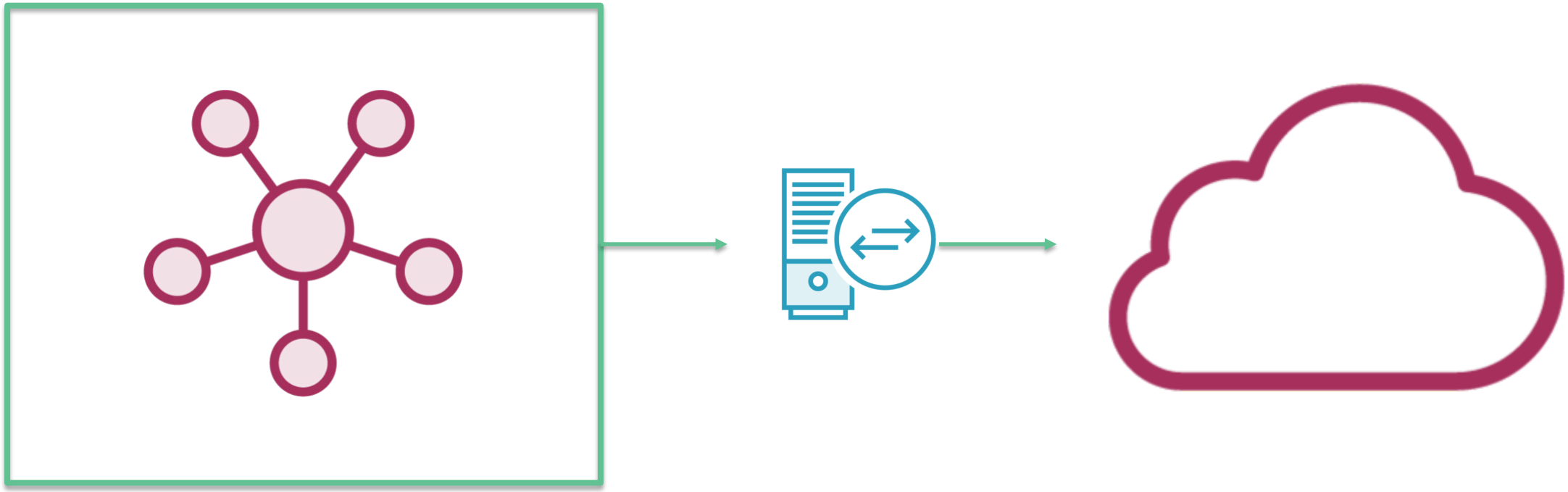
"I don't always use air gapped networks, but when I do, they are almost always still connected to the internet in some way."

What an Air Gapped Network Is Not

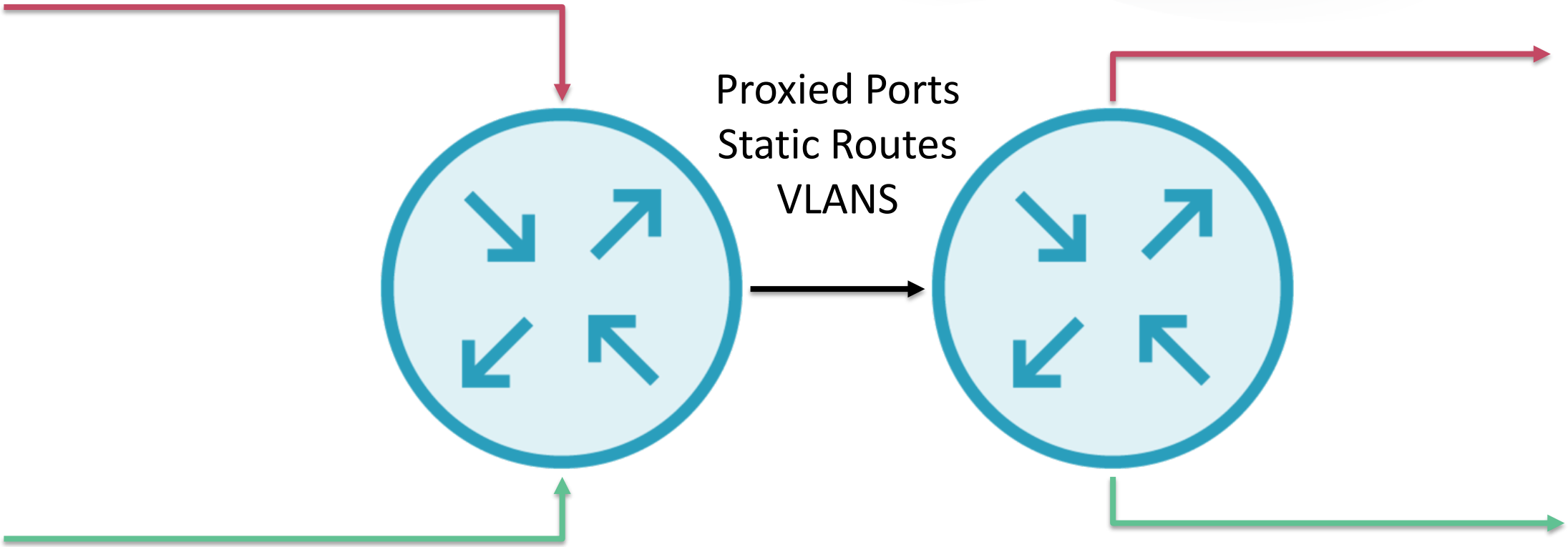
Air Gapped Network is not truly disconnected from everything.



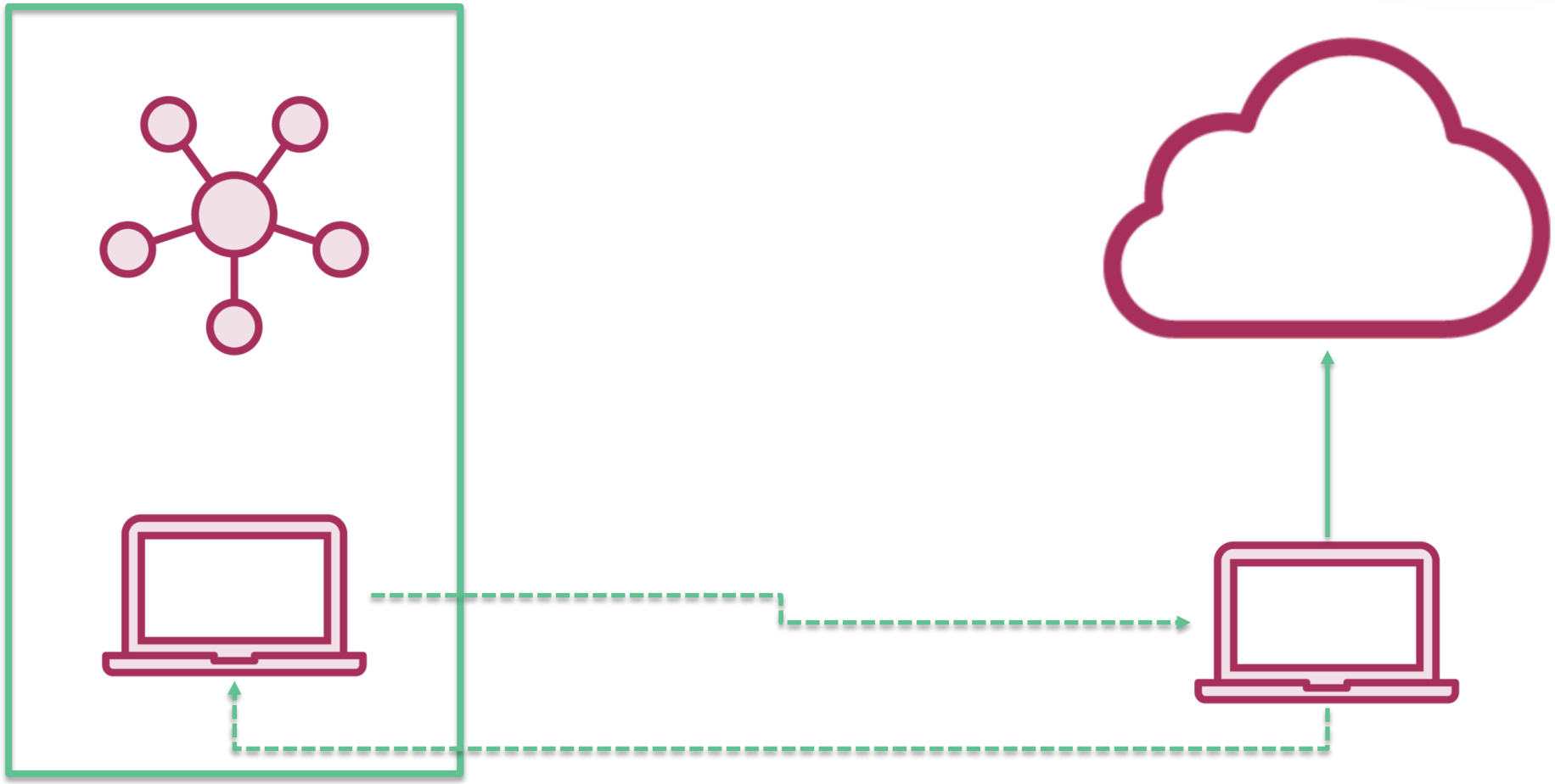
Cross Domain Solutions



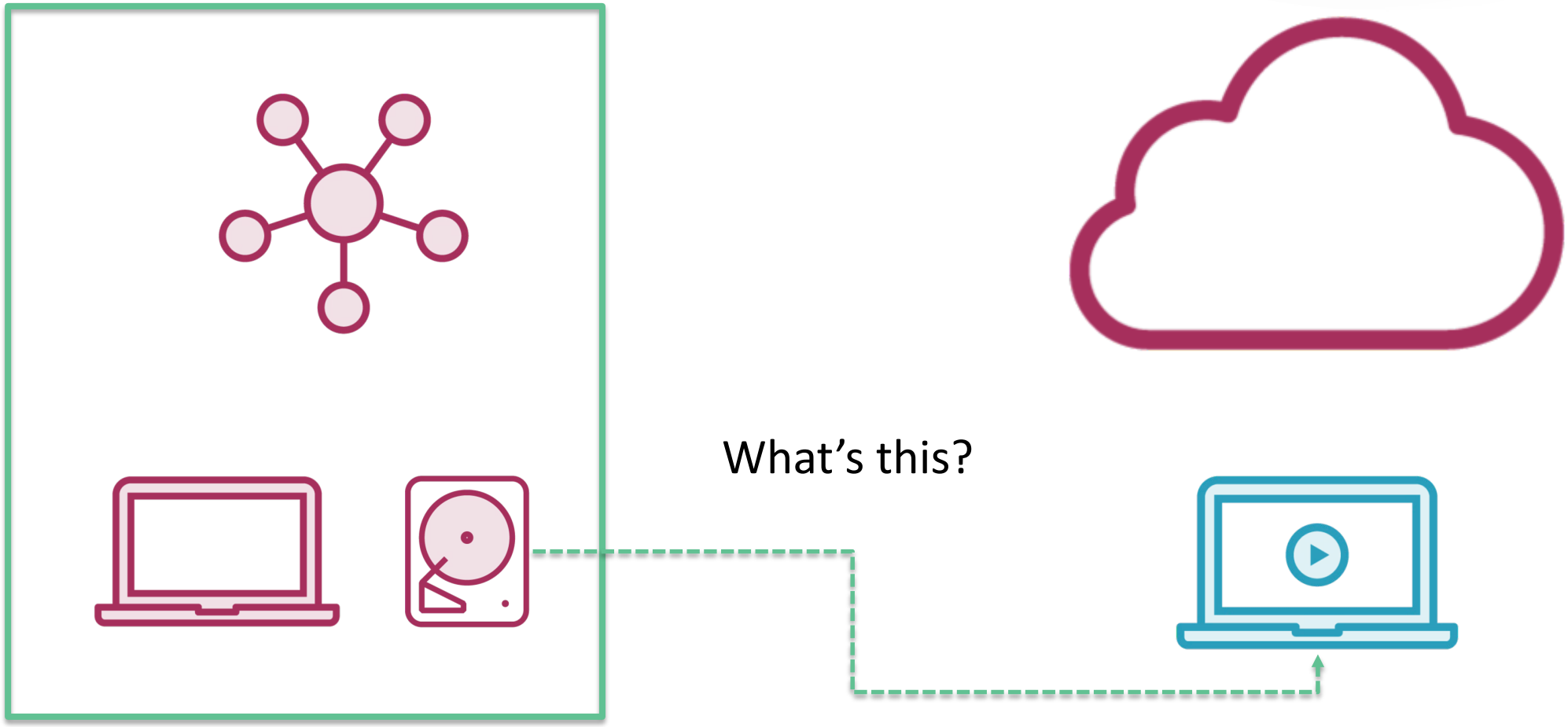
Sharing of Infrastructure



Intermittent Endpoint Connections



Accidental Hardware Use



Characteristics of an Air-gapped Network

What is different?

- No direct download from a stager from an attack like phishing
- Much less exposure to commodity malware
- No threat of internet drive-by type concerns
- Users can't download from the internet

What is the same?

- Still uses software, that needs to be updated…from the internet.
- Still has users
- Shares spaces and sometimes network equipment with non air gapped networks
- Generally exists in the same format as any other environment

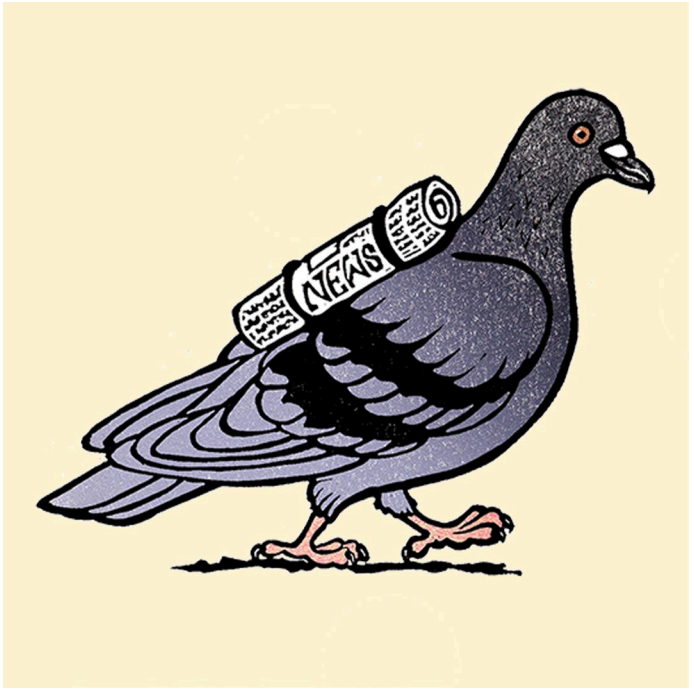
Not All That Safe

Common issues

- Not heavily monitored
- More incentive for advanced adversaries
- Lagging or no updates

Out of Band

Out-of-band is activity outside a defined telecommunications frequency band, or, metaphorically, outside some other kind of activity.



Side Channels

A **side-channel attack** is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself.

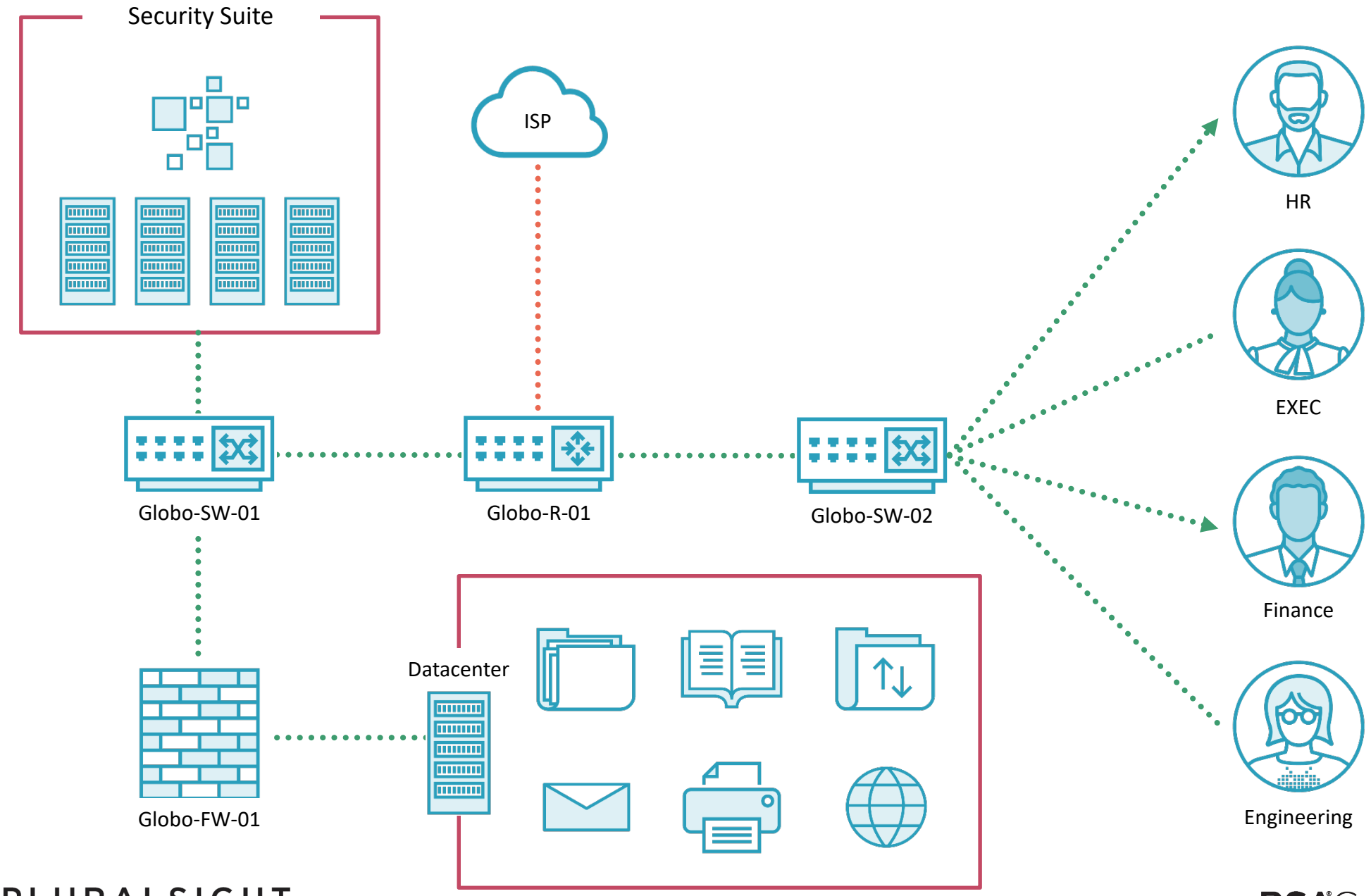
Execution of commands:
Randblob (100)
Randblob (1,000,000)

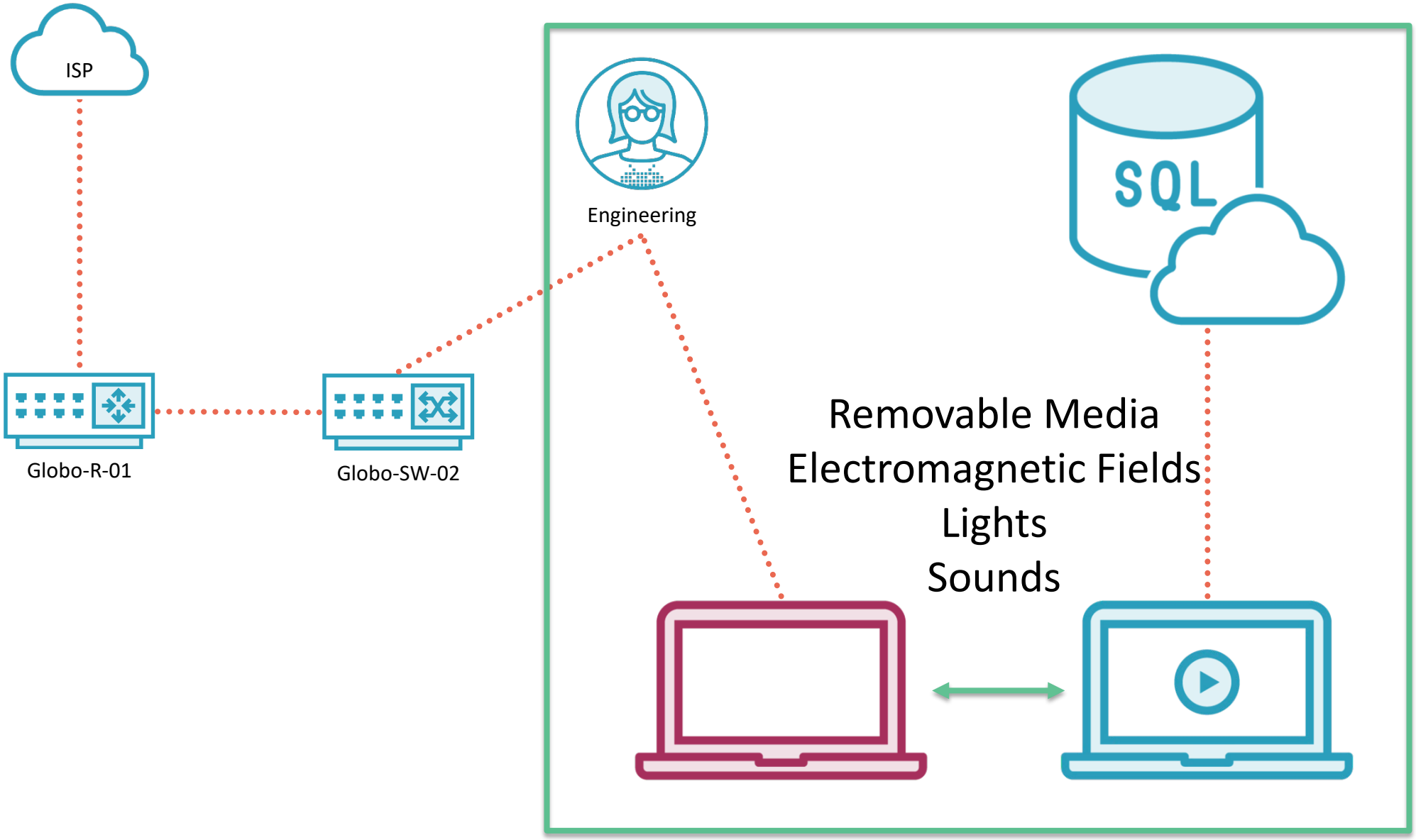
Response Timing Analysis:	1ms vs 100ms
Power Usage Analysis:	1w vs 100w
Sound Variation Analysis:	+1db vs -60db
Optical Queue Analysis:	1ms Blink vs 10x 1ms blink

RSAConference2020

Setting the Scene

Prime your imagination


Security Suite
ISP
HR
EXEC
Finance
Engineering
Globo-SW-01
Globo-R-01
Globo-SW-02
Globo-FW-01
Datacenter


ISP
Globo-R-01
Globo-SW-02
Engineering
SQL
Removable Media
Electromagnetic Fields
Lights
Sounds

Still Connected

- Updates – software supply chain
- Removable Storage – Could include hard drives.
- Based on realities of management and people. A policy against something does not mean it never happens.
- Hardware, computers, software, network jacks in wall, all sorts of physical situations that offer attack vectors
- Simply by sharing the same space, other physics comes into play for advanced out of band communication

RSAConference2020

Basic Side Channels

The pumpkin spice of out of band communication

USBs

“DO NOT SHARE”

Agent.btz

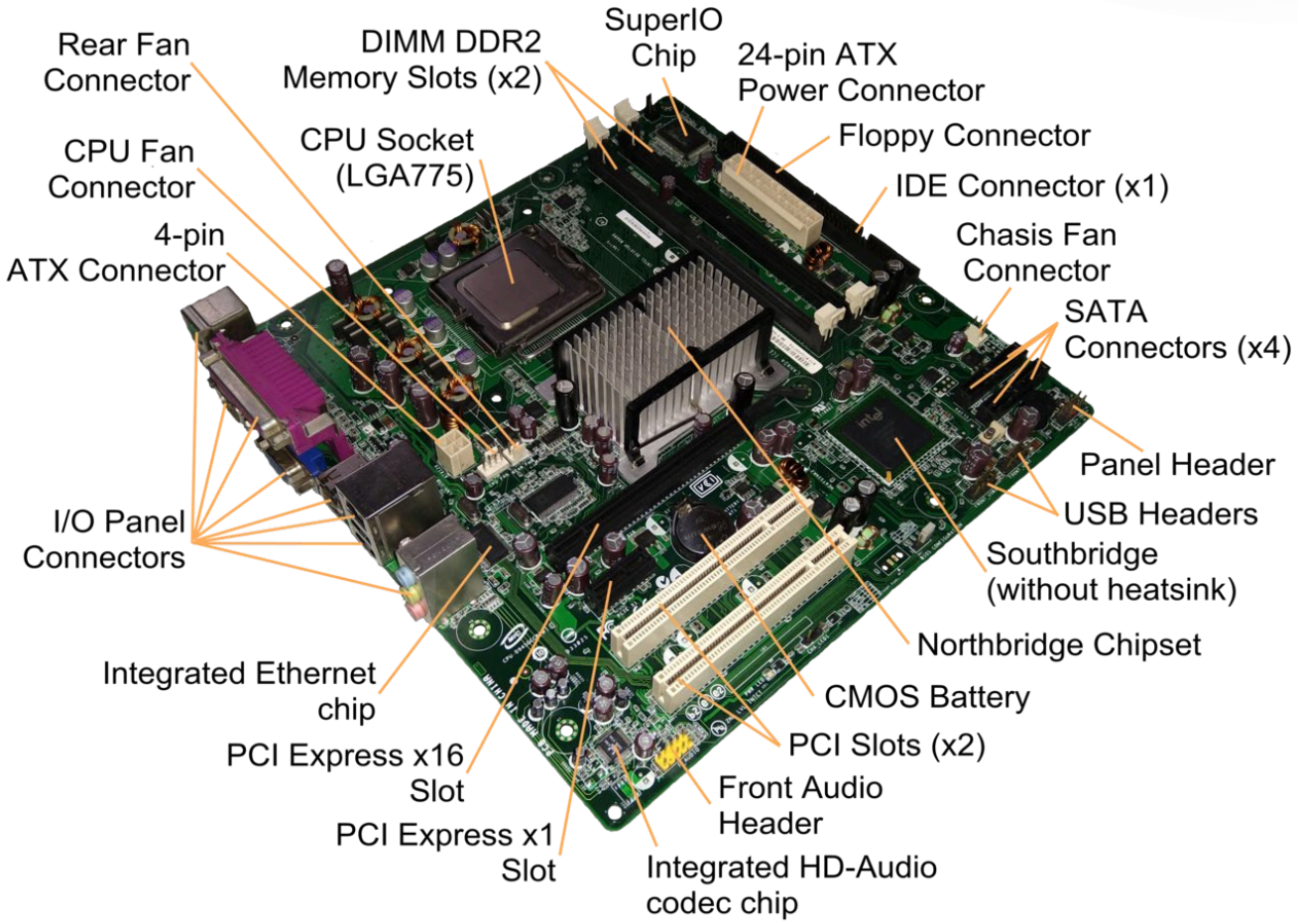
Still Using CD/DVD/SD Cards?

Is this better than USBs?

Why it is totally not any better.

- Nearly every desktop computer and server has a CD/DVD writable drive.
- There are different security policy standards for each of these devices
- No good way to implement BIOS level lock out of these devices at scale
- Can hold just as much data
- CD/DVDs sit inside the computer

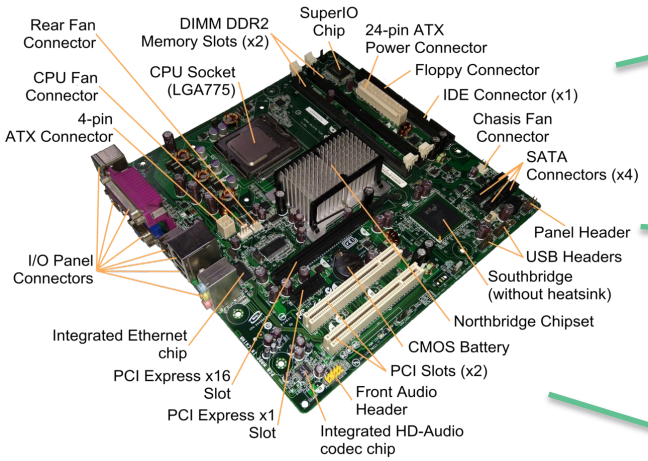
Every Component Is an Attack Vector



Every Component Is an Attack Vector

DMA – Direct Memory Access

"It's a feature"



BIOS

github.com/rdebath/viruses/blob/master/virus/k/k-cmos.asm

PCI-E

github.com/ufrisk/pcileech

Device Firmware

https://www.kaspersky.com/blog/equation-hdd-malware/7623/

RSAConference2020

Advanced Side Channels

Defining the problem and the physics

What I Am

- Pluralsight Author and Researcher
- Air National Guard
- National Exercise Red Team Lead
- Red/Blue Consultant

What I Am Not

- Exploit developer
- One man APT
- Highly funded research lab
- Machine Learning Scientist
- MIT or equivalent Grad

Credit where credit is due

- Dr. Mordechai Guri (Advanced Cyber-Security Research Lab)
  - https://cyber.bgu.ac.il/advanced-cyber/airgap
    - **BRIGHTNESS: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness**
    - **PowerHammer (exfiltrating data through power lines)**
    - **MOSQUITO (Acoustic)**
    - **ODINI (Magnetic)**
    - **AirHopper (Electromagnetic)**
    - **BitWhisper (Thermal)**
    - **DiskFiltration (Acoustic)**
    - **Fansmitter (Acoustic)**

Alternate Means of Communication

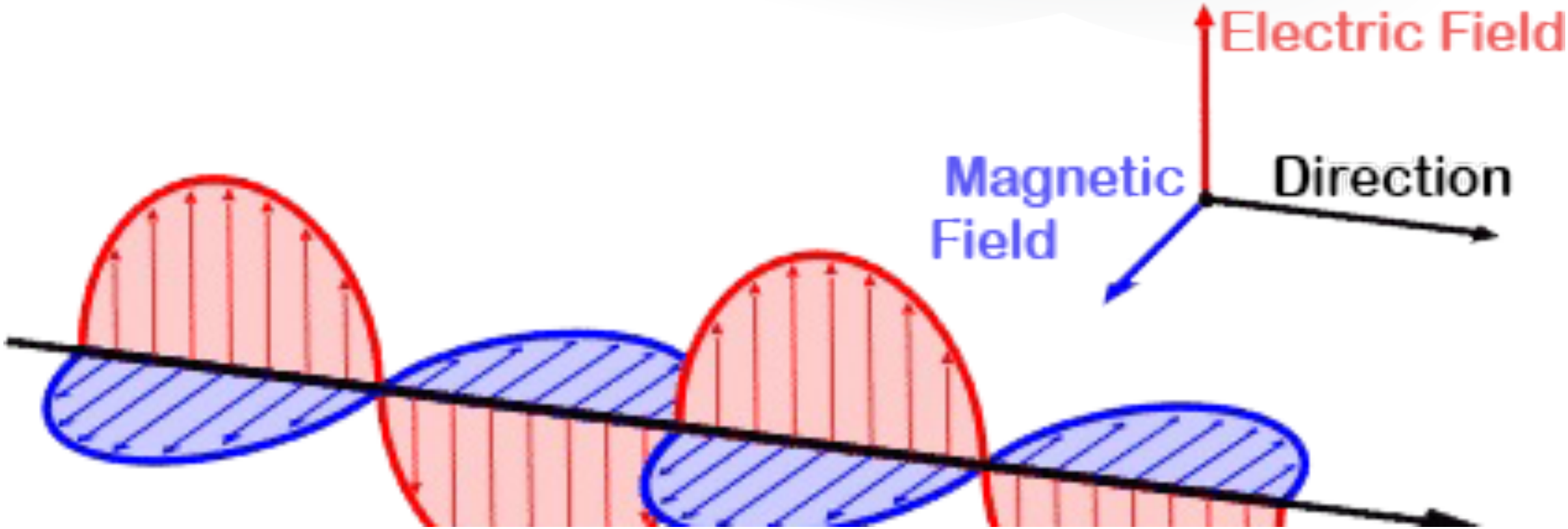
Electromagnetic Waves

- Visible Light
- Magnetic fields & Radiation
- Radio Waves
- Infrared
- Heat via temperature

Mechanical Wave

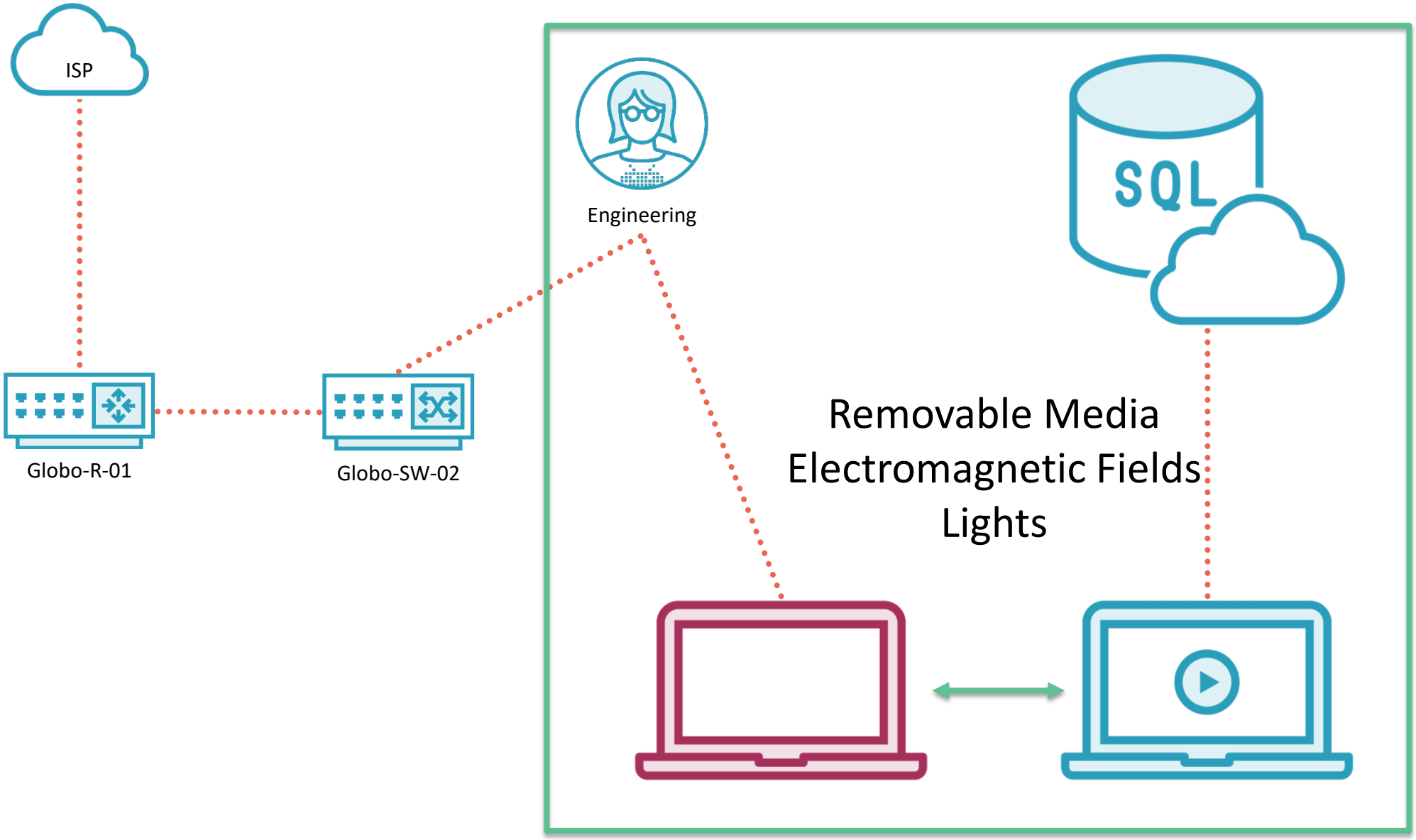
- Vibrations - Accelerometer
- Sound/Audio Waves

What Is an Electromagnetic Wave?



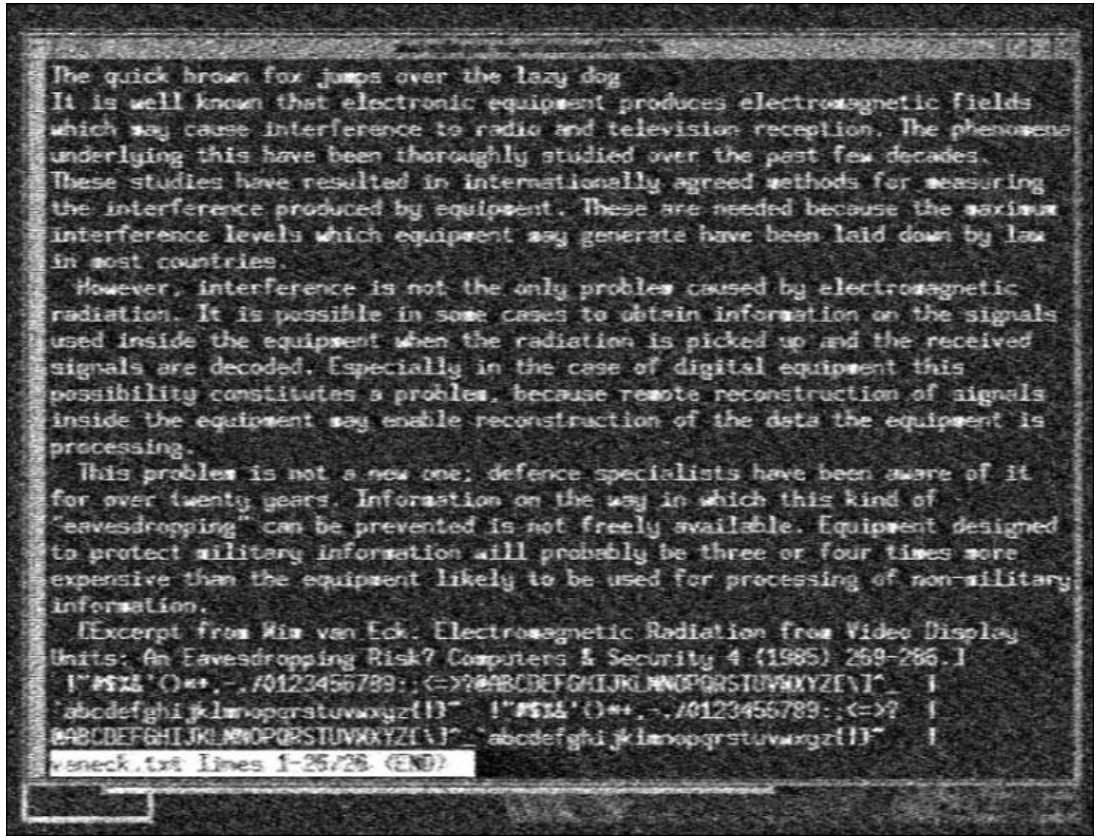
GENERATED FROM THE MOVEMENT OF ELECTRONS

Computers operate entirely on the movement of electrons and all that movement generates electromagnetic fields and radiation


ISP
Globo-R-01
Globo-SW-02
Engineering
SQL
Removable Media
Electromagnetic Fields
Lights

Electromagnetic Radiation

10m with two offices in between



Van Eck Phreaking

- https://www.cl.cam.ac.uk/~mgk25/iss2006-tempest.pdf
- Van Eck Radiation
- Espionage only
- CRT & LCD monitors at risk
- TEMPEST & Faraday Cages

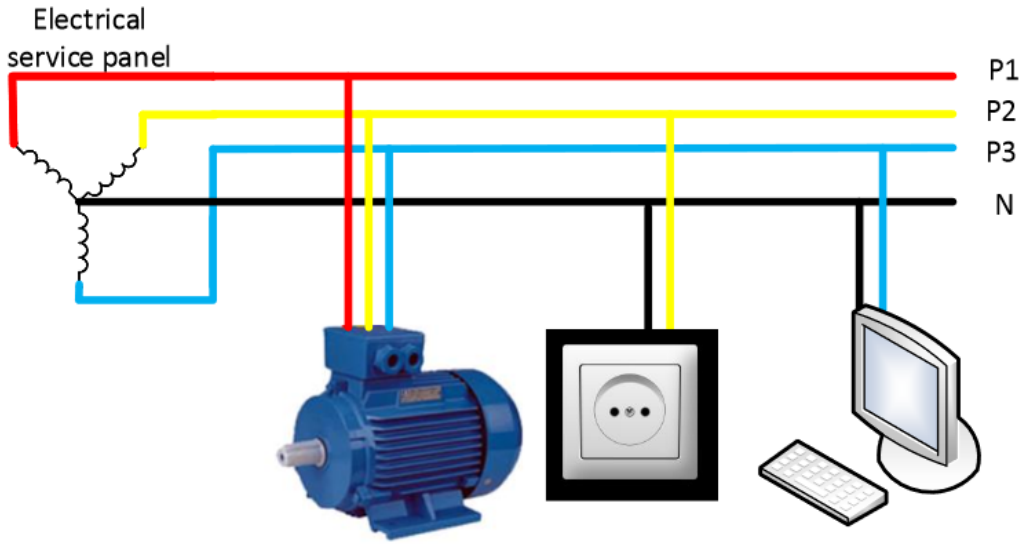
Blinking Lights and Drones

Lights on every device

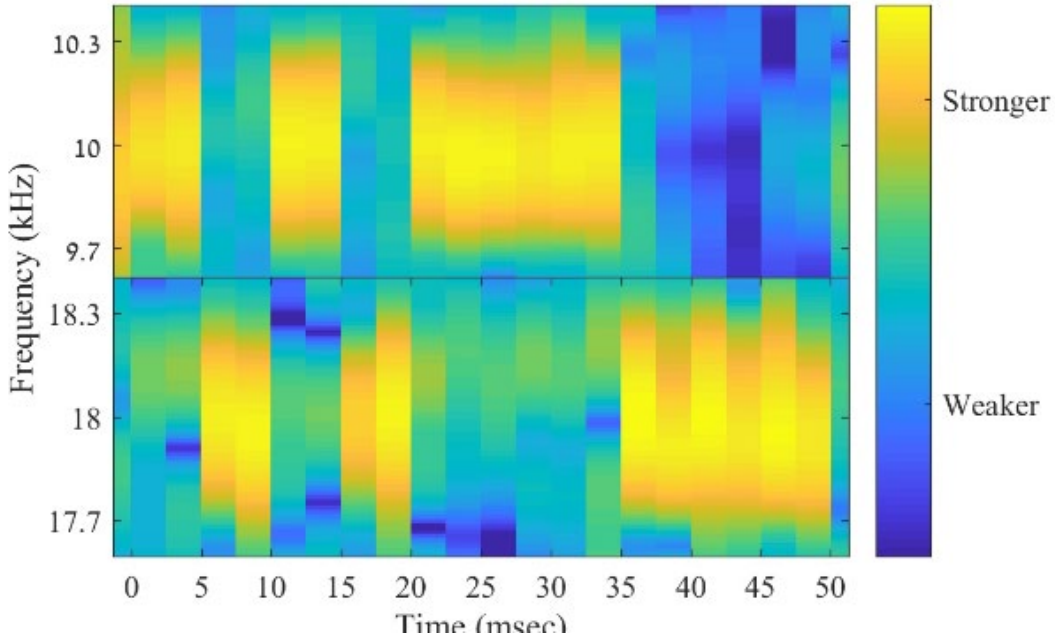
- Lights on outside of computer blink when the hard drive is accessed
- This pattern of blinking can reveal information about the data being processed
- Drones read the light with high def cameras through a window
- https://www.wired.com/2017/02/malware-sends-stolen-data-drone-just-pcs-blinking-led/

EM Enables Reading Data Through Power

Power circuits are like a network



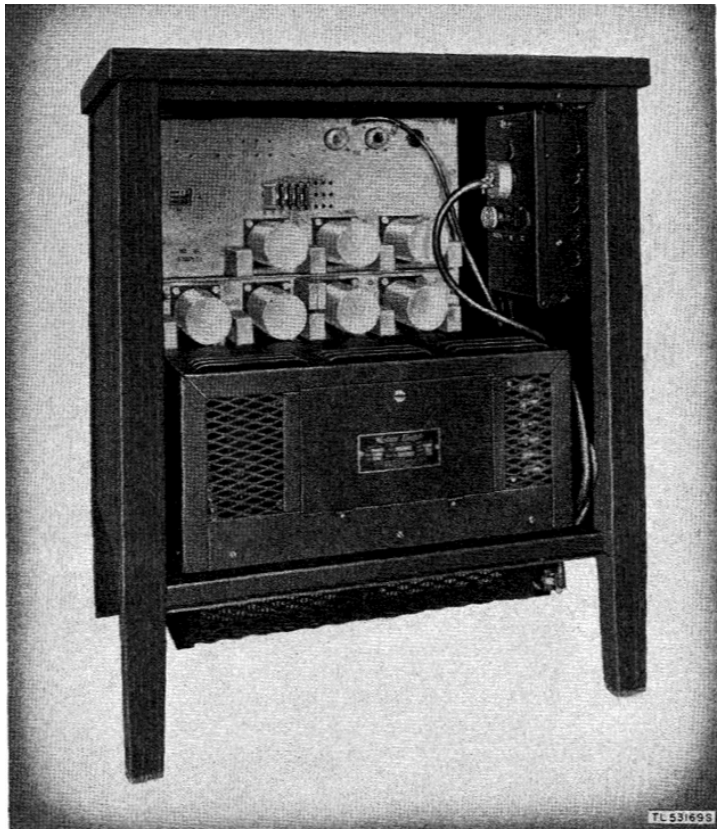
Transmitting binary



Don’t we have people for this?

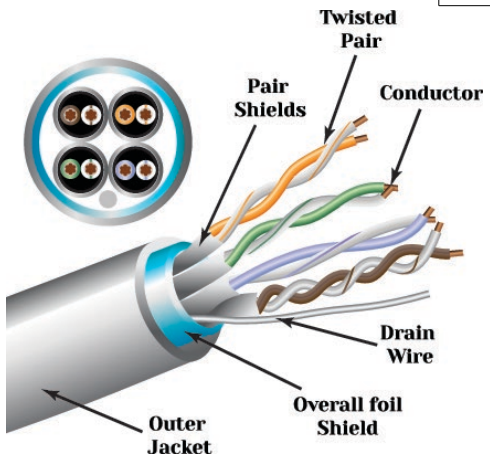
TEMPEST
Telecommunications Electronics Materials
Protected from Emanating Spurious Transmissions

- Shielding of electronic components
- Specification of “safe distances”
- Red/Black implementation

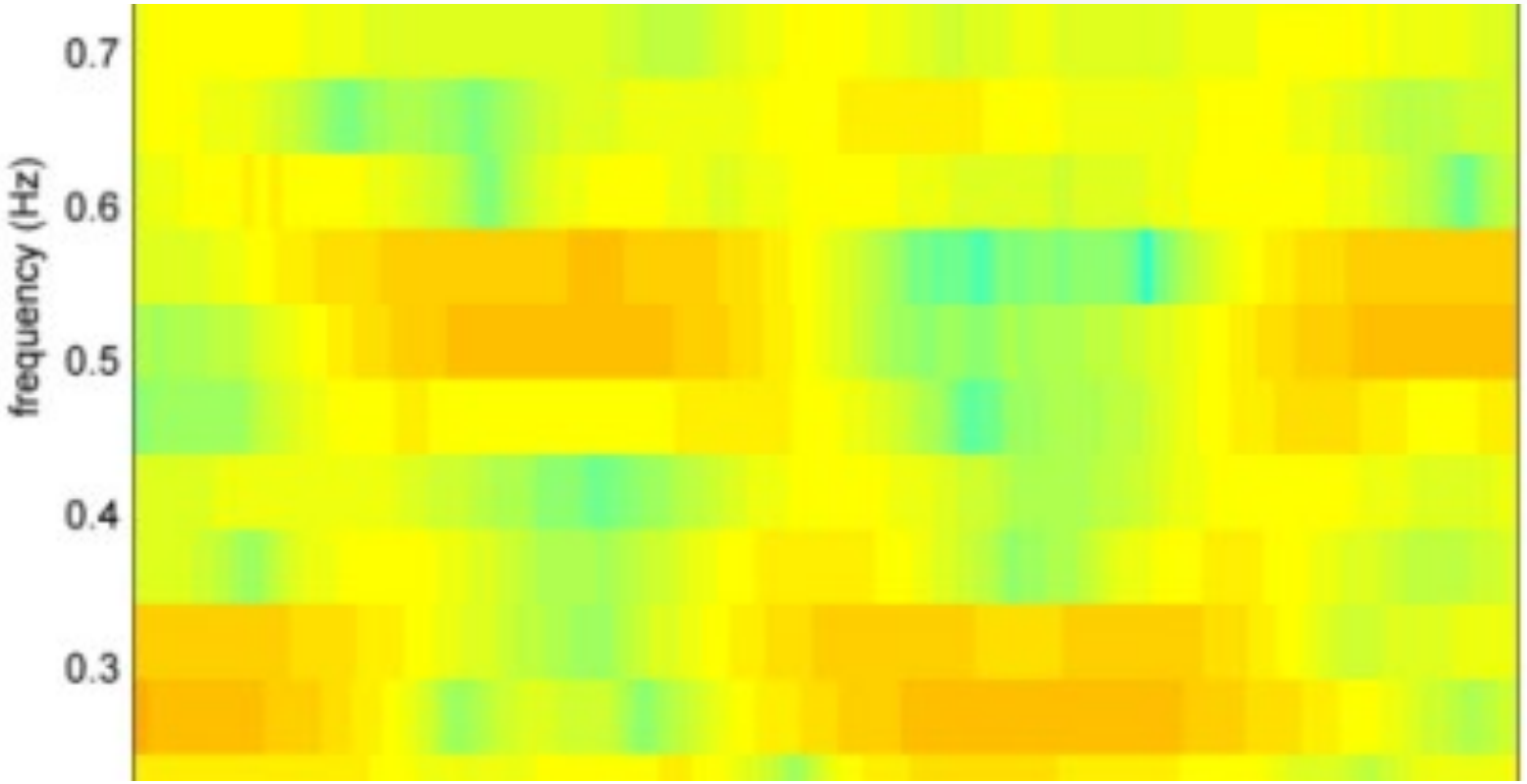


Bell 131B2 Mixer used to XOR signals during WWII

Protections

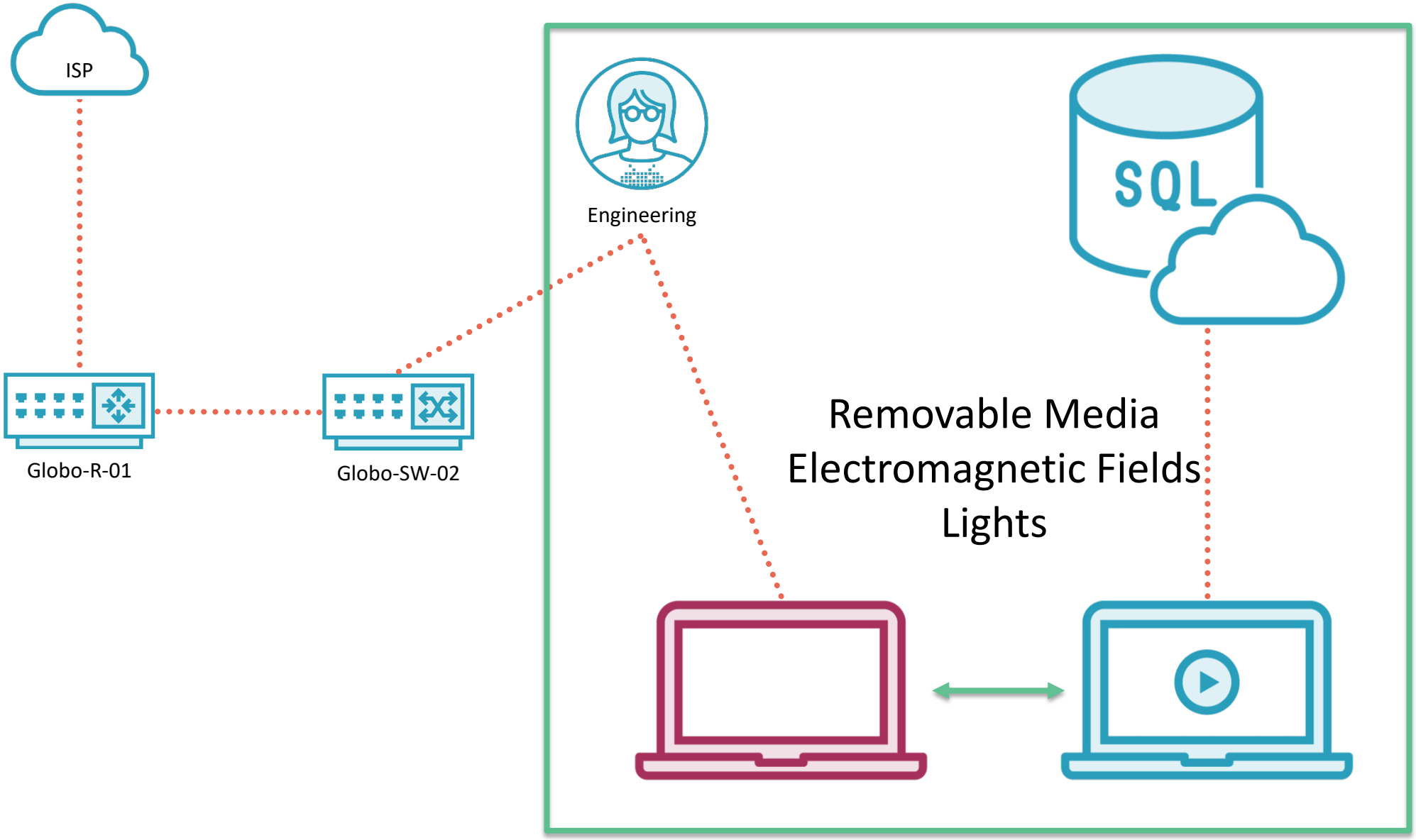


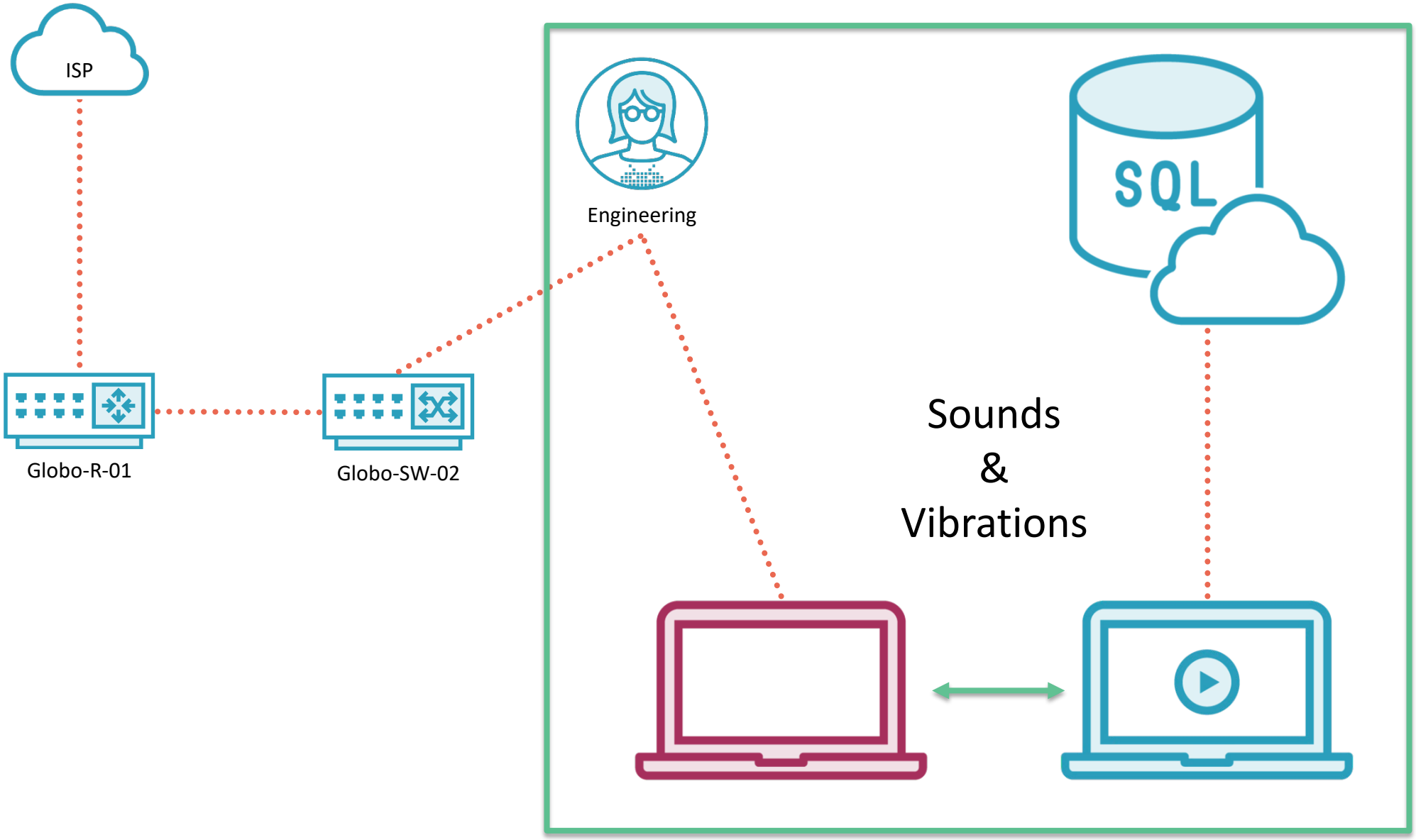
Magnetic Field Reading



FARADAY CAGE IS NOT THE TOTAL ANSWER

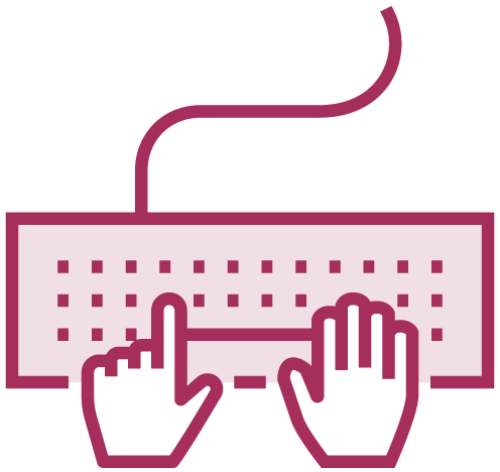
https://www.fanaticalfuturist.com/2018/05/hackers-find-a-way-to-neutralise-faraday-cages-to-exploit-air-gapped-systems/ - https://cyber.bgu.ac.il/advanced-cyber/system/files/MAGNETO_0.pdf


ISP
Globo-R-01
Globo-SW-02
Engineering
SQL
Removable Media
Electromagnetic Fields
Lights


ISP
Globo-R-01
Globo-SW-02
Engineering
SQL
Sounds
&
Vibrations

Mechanical Waves Vibrations

- Stealing passwords or keylogging using the accelerometer on a phone sitting on a desk
- https://gcn.com/articles/2011/10/18/smart-phone-sensors-steal-keystrokes.aspx

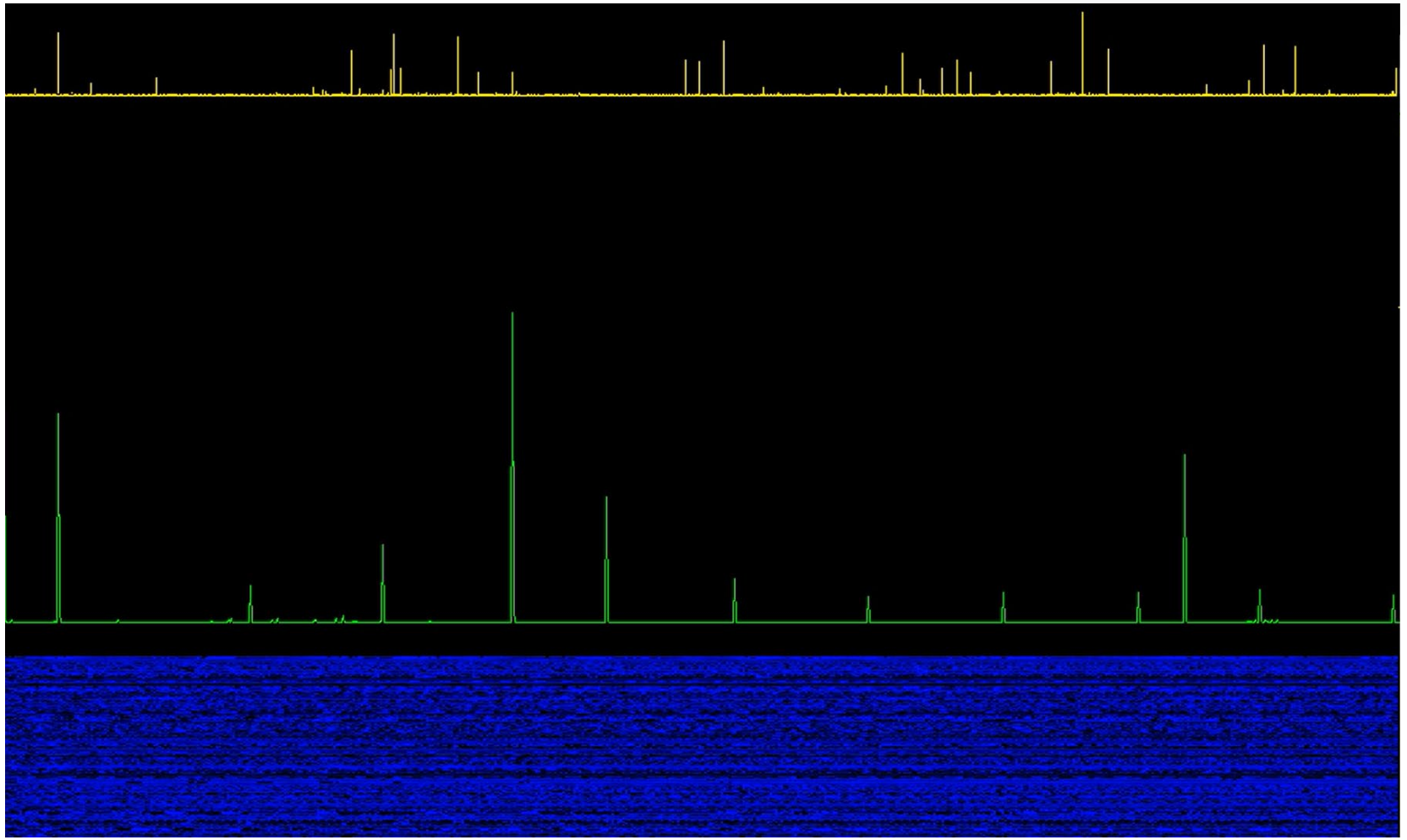


RSAC2020!

Sound Is a Mechanical Wave as Well

- Transmitting data over sound
- Fans and speakers of all kinds
- Using sound to destroy hard drives
- Listening to conversations via spinning hard drives
- Ultrasonic capabilities outside the range of human hearing

Hard Drive Spin Interruption



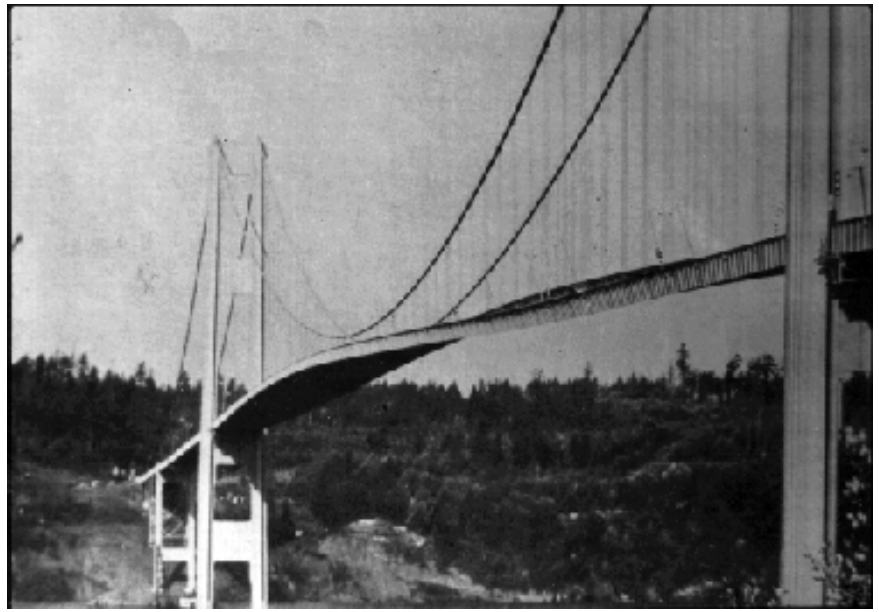
IO Latency

```
 0: 148.749104 ms
+1: 1582 ns
+2: 949 ns

-1: 945 ns
 0: 55.786925 ms
+1: 1710 ns
+2: 968 ns

-1: 938 ns
 0: 32.434953 ms
+1: 3638 ns
+2: 971 ns

-1: 945 ns
 0: 31.674332 ms
+1: 2287 ns
```

https://github.com/ortegaalfredo/kscope

Destructive Mechanical Resonance

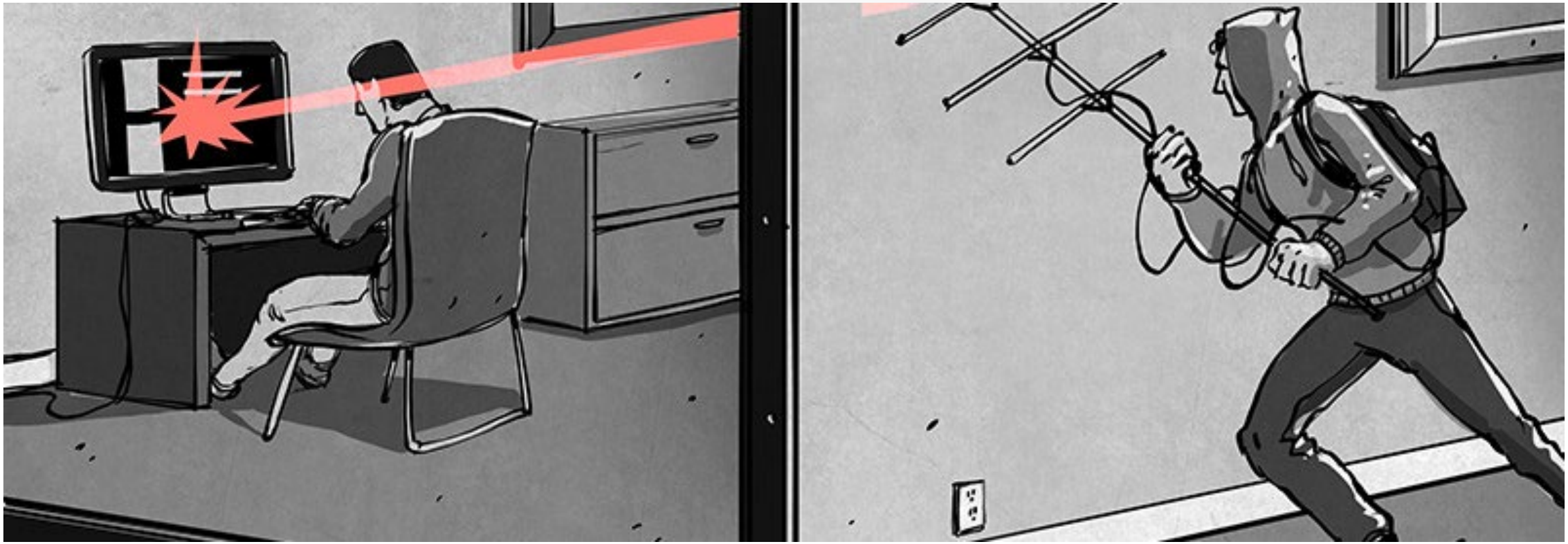
Tacoma Narrows Bridge



Leveraging Hard Drive Resonance

- After 1 minute of inoperability hard drives are dropped from the operating system
- Potential for physical destruction of spanning platters
- Kscope project uses the hard drive interruption feedback to zero in on resonant frequency

Lack of Understanding Lessens Compliance



SOMEONE ALWAYS WILL DO IT ANYWAY

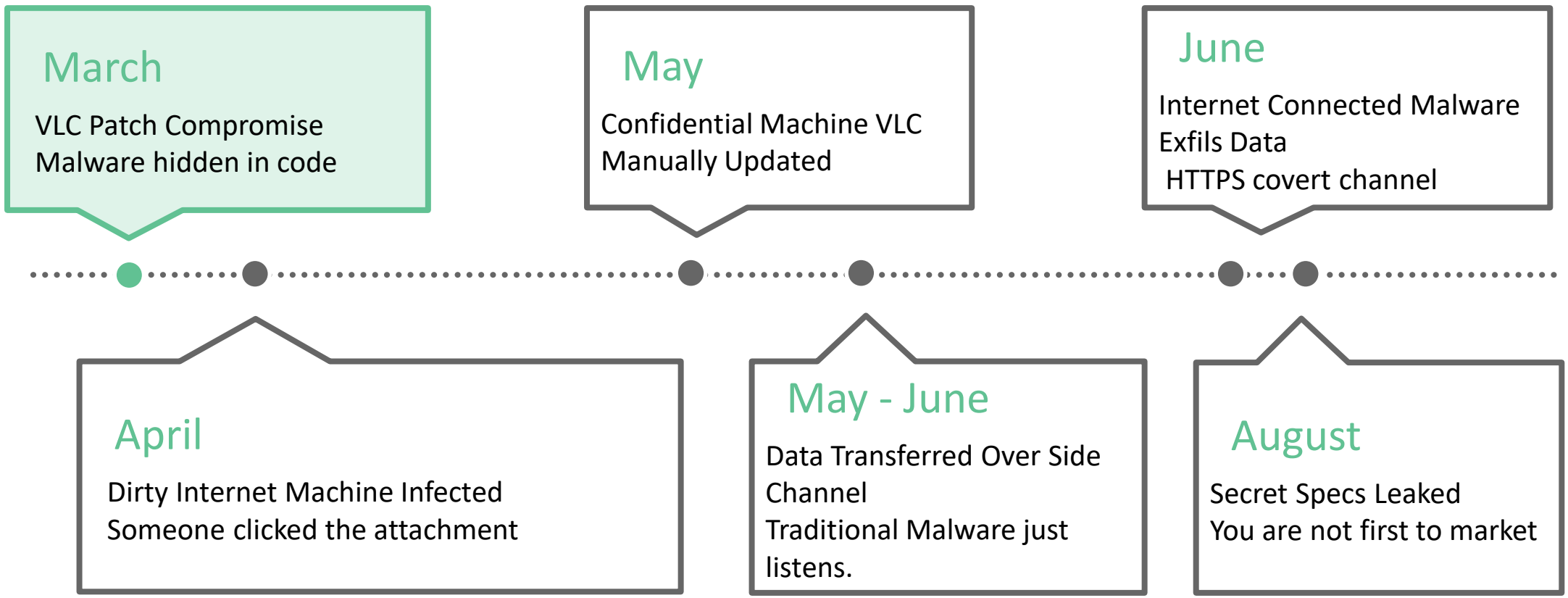
Adversarial Thinking Depends Upon Inevitabilities of Human Nature. Human behavior is a dumpster fire.

RSAConference2020

Chain of Compromise

How is this really done?

Timeline of Events



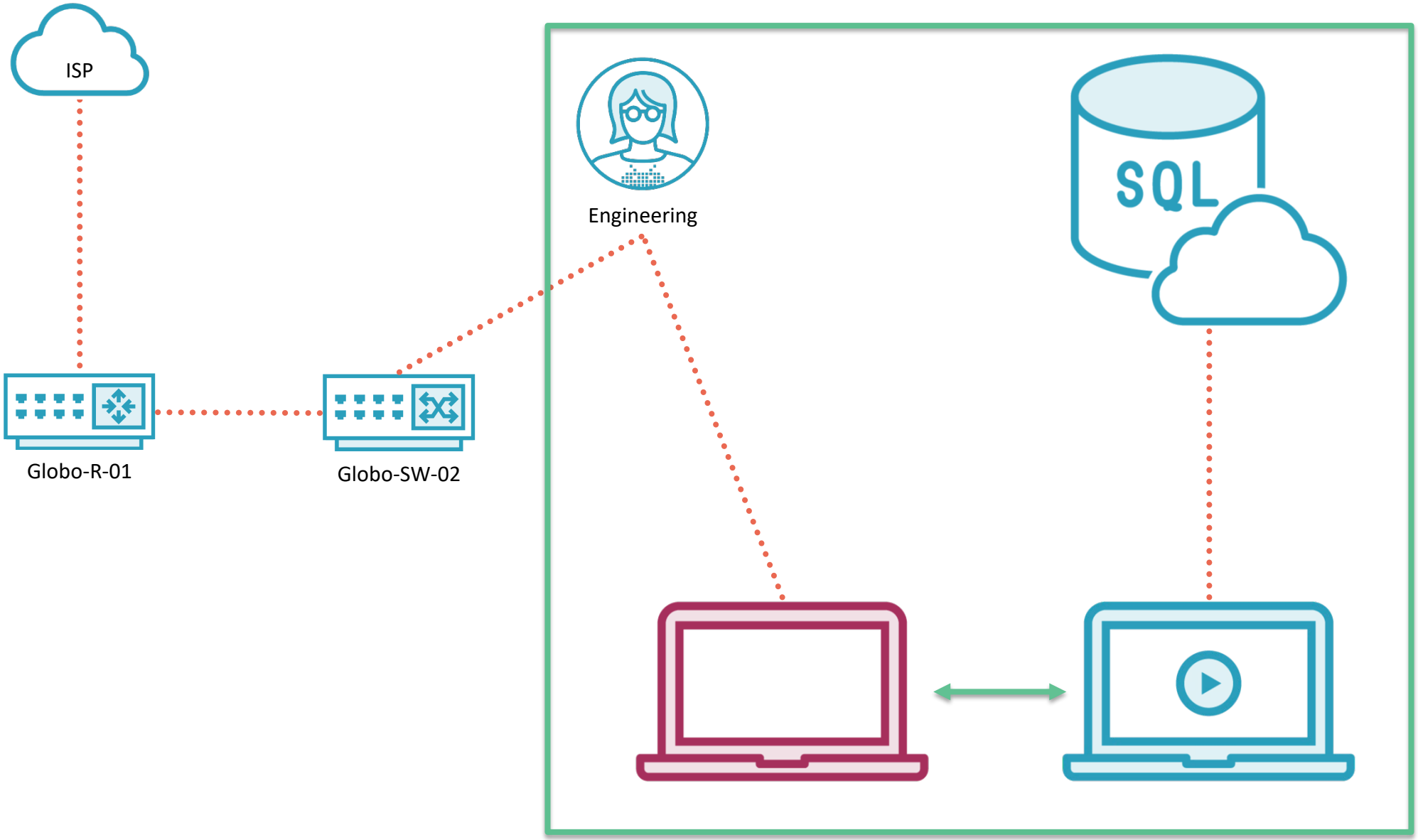

ISP
Globo-R-01
Globo-SW-02
Engineering
SQL

Diagram Movement of How the Fan Comes into Play

Components of a Successful Attack

Connected Network

- Pre-compromised devices in the correct room
- Can be the server room if rack adjacency is achieved
- Microphone/listening capability
- C2 channel established for exfil

Air-Gapped Target

- Compromised, manual updates
- In the same room as connected compromised machine
- Ability to operate autonomously
- Access and recognition of sensitive information
- Access to correct models/fans

RSAConference2020

POC Musical Fans

Using sound to hop air gaps

Transmitting Data with Sound

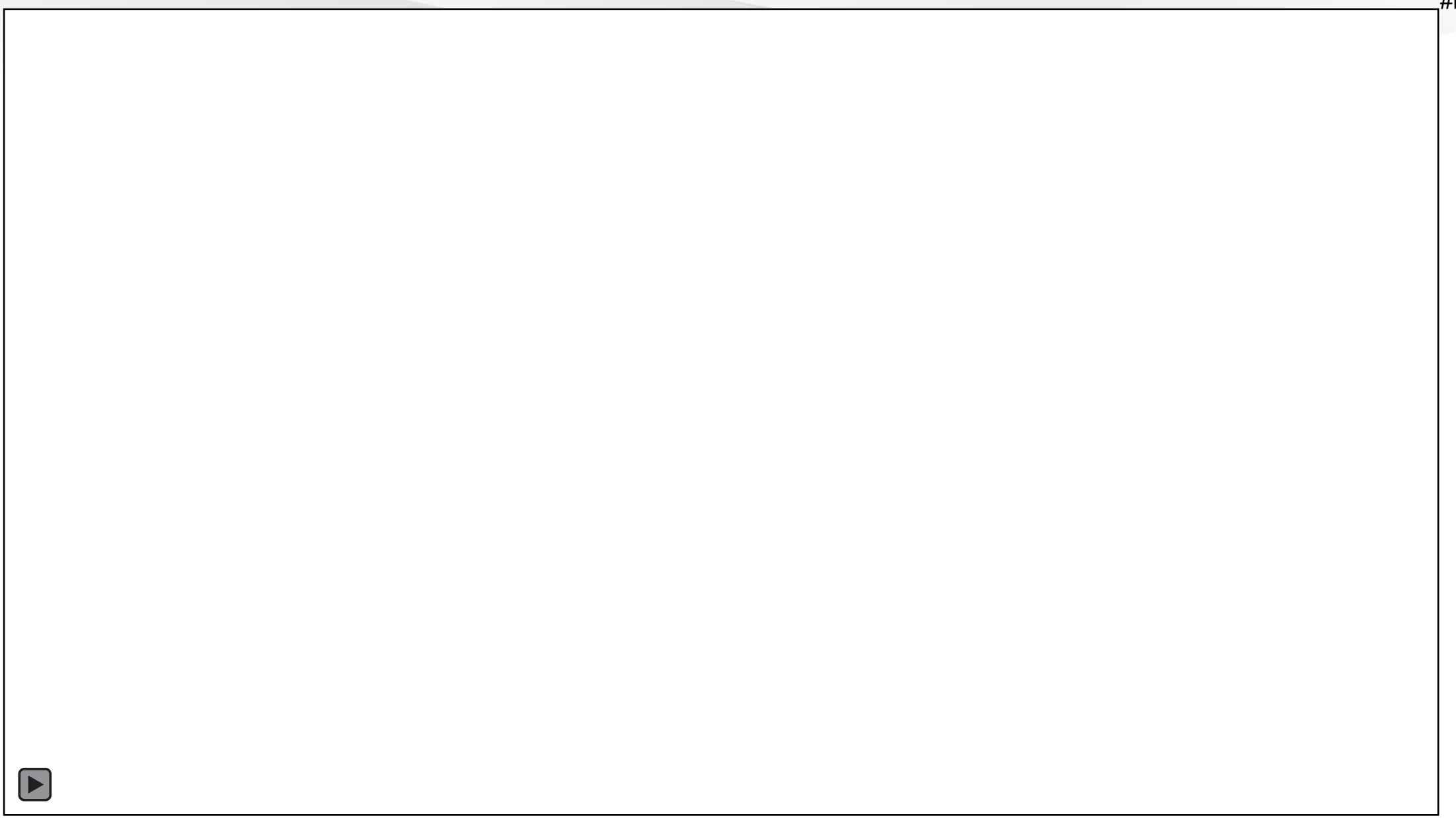
- Something that makes noise
- Data to be transmitted
- Encoding
- Transition from digital to mechanical waves

Receiving Data over Sound Waves

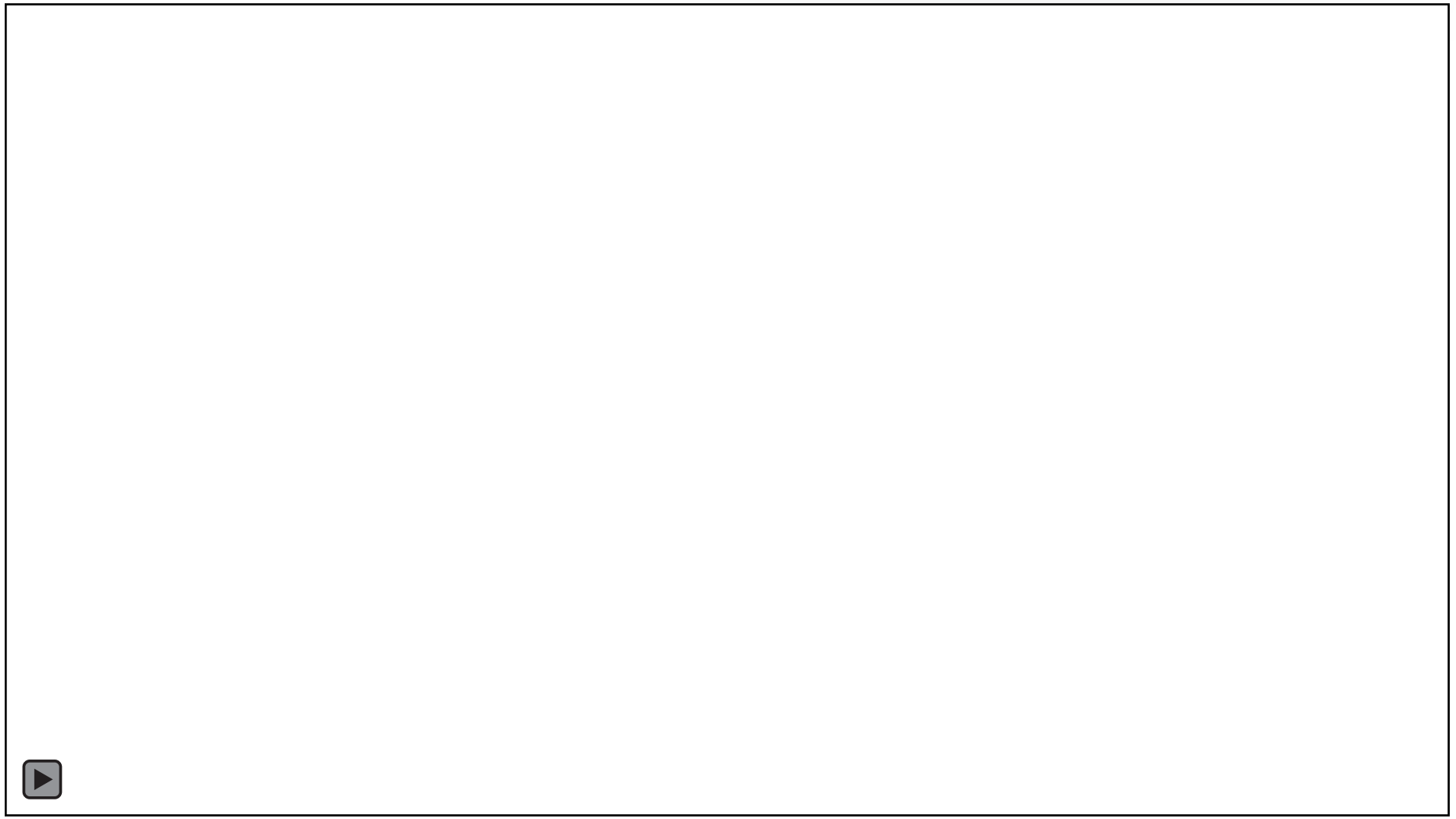
- Think Morse code
- A bit more complicated than it would seem
- Recording device in range
- Is not required to be done at the time of reception
- Could be modified for efficiency, accuracy and sensitivity with team of machine learning scientists

Recorded Demos

If you are reading this…then my worse fears have come true and my live demos have failed. ~AMR



Receiving Data via Sound Waves



Receiving Data over Sound Waves

- Research has been done on this with a tool called fansmitter
- The blowing hot air demonstration achieved a transfer speed of 30 bits per minute
- Developed with a total of 25 working hours by one person
- Also my code is free for you to use: https://github.com/arosenmund/blowinghothair
- All developed in a home lab

RSAConference2020

What Is to Be done?

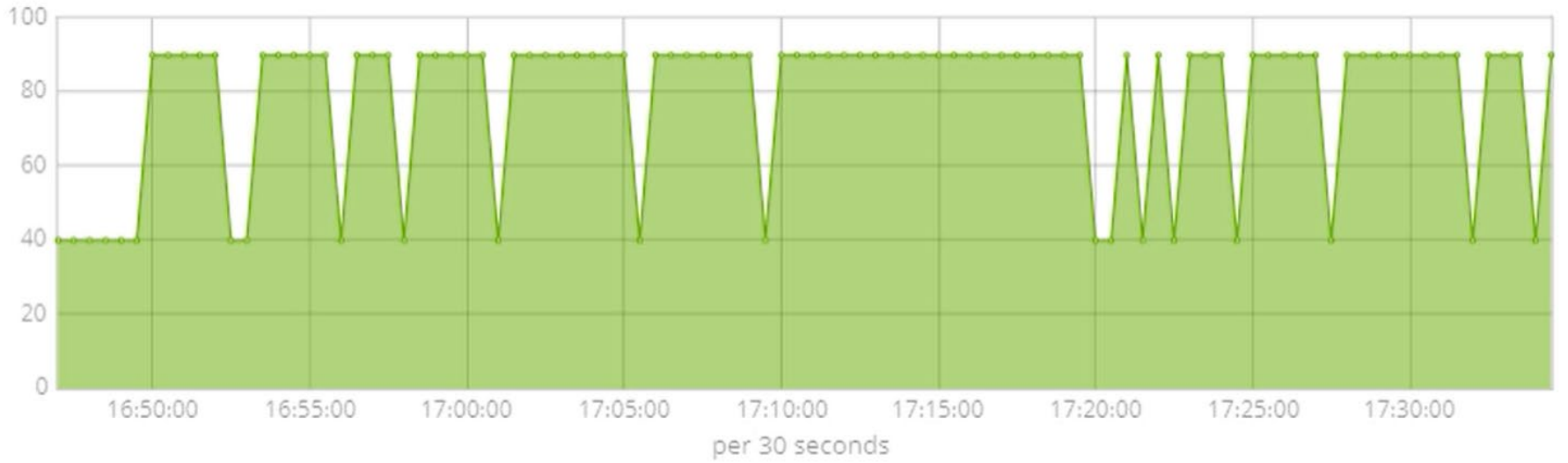
Defending against air gap hoping side channels

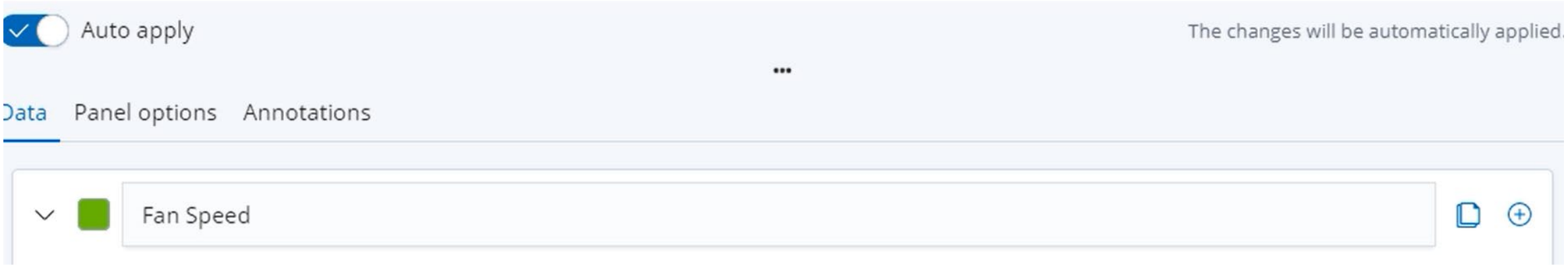
Detections 1

- Variations in fan, light or power that occur in a digital fashion (high/low) and in a timing that would indicate data transfer that deviates from established baseline.
- Mitre Att&ck Technique
- - T1052: Exfiltration over physical medium(amended)
- - T1195: Supply chain compromise(software)

**Used modified GPUbeat developed mostly by eBay to monitor NVidia fan speed in elastic stack. Also available in GitHub.*

Monitoring Fan Speeds



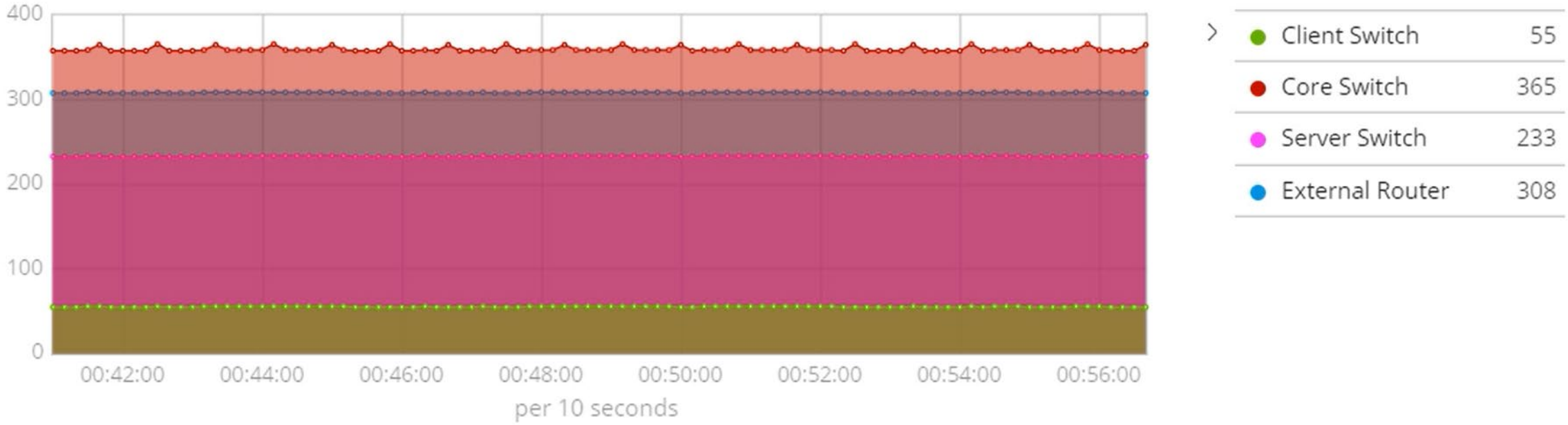


Detections

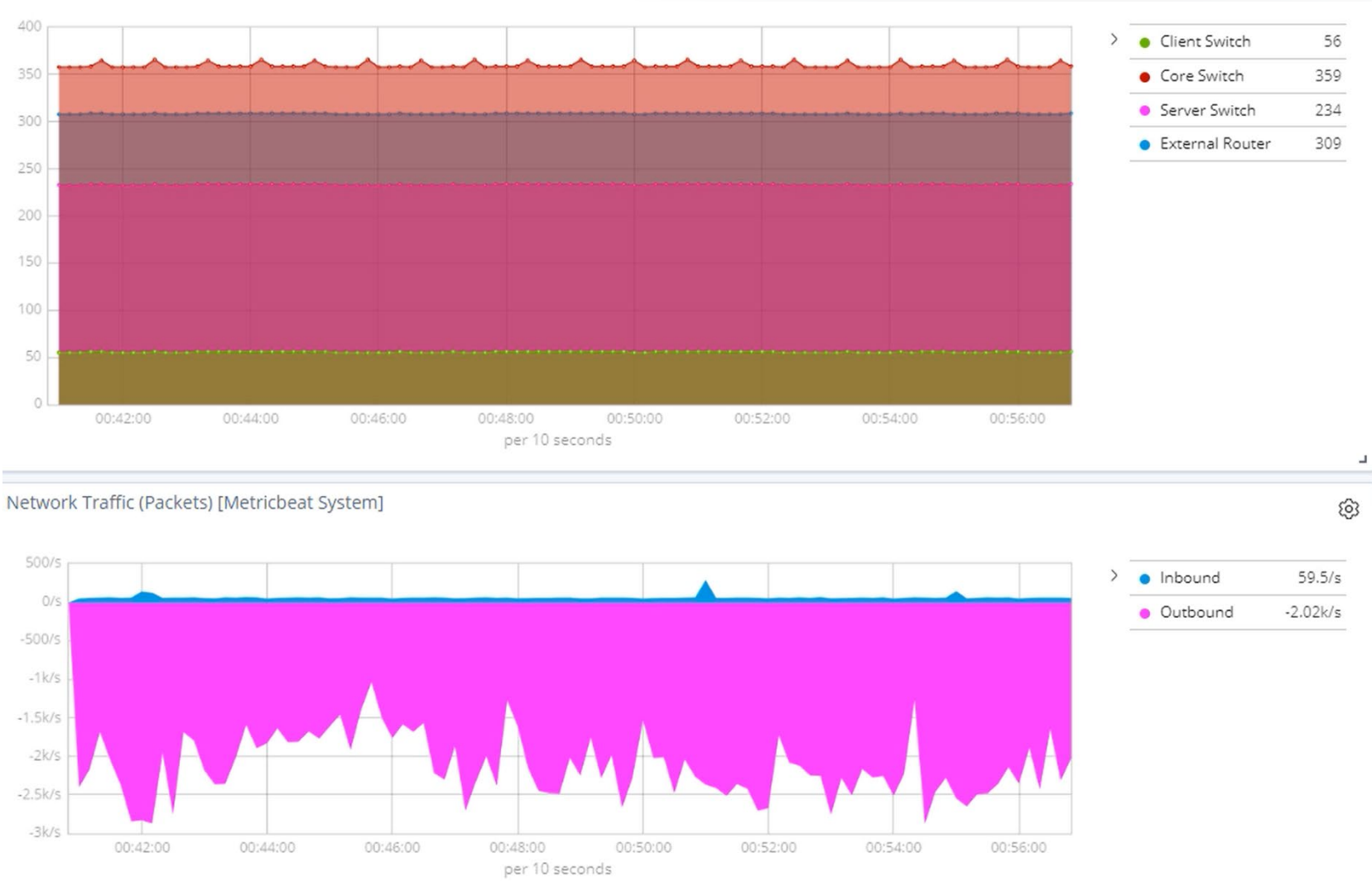
- Power fluctuation differences across populations of the same model switch/router devices not attributed to attached device network activity, cross referenced with device vendor and batch for correlations.
- **Mitre Att&ck Technique**
- **- T1195: supply chain compromise(hardware)**

Monitoring Power vs. Network Spikes

Time Series | Metric | Top N | Gauge | Markdown | Table

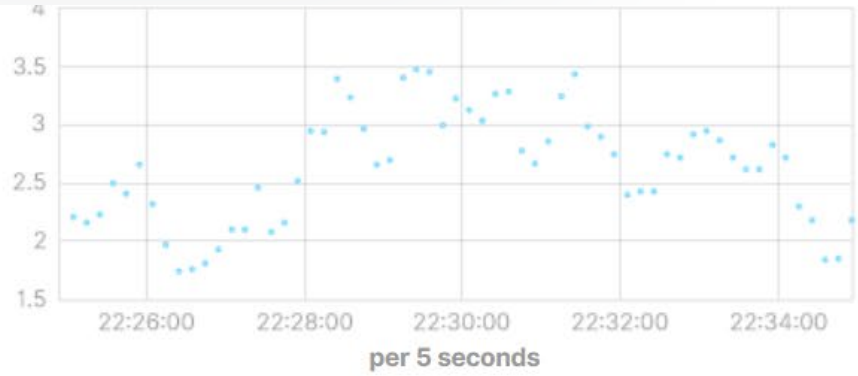


Monitoring Power vs. Network Spikes

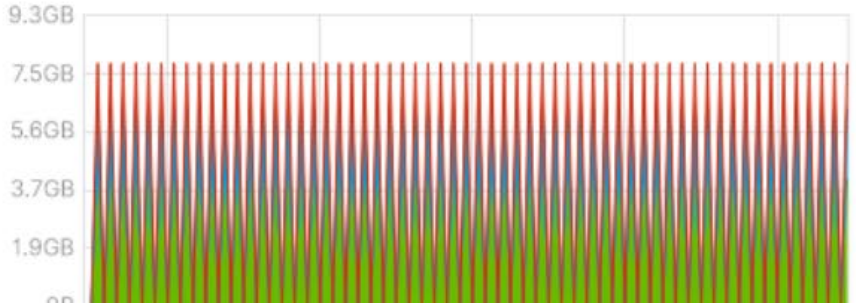


CPU Core load magnetic resonance detection

user	310.9%
system	2.3%
nice	0%
irq	0%
softirq	0%
iowait	0%



Memory Usage [Metricbeat System] ECS



Used	1.4GB
Cache	2.3GB
Free	4.1GB

Disk IO (Bytes) [Metricbeat System] ECS

THIS IS MUCH MORE DIFFICULT THE PRACTICAL SCALES OF TIME ARE SMALLER

Used “stress –c 4” on same schedule as the fans to transmit the same data: captured with metric beats.

Summary

- Architecture and policy decisions impact success of air gap implementation
- Basic out of band attack vectors go well beyond USBs
- Advanced attacks are likely already in use and there is no single off the shelf product to protect you
- Monitoring deviations from baseline is and correlating events for added context is key

Apply these concepts

- Implement monitoring on Air Gapped Networks with potential for side channel data exfiltration ML – do this now
  - https://github.com/arosenmund/blowinghothair/tree/master/detections
  - https://app.pluralsight.com/library/courses/security-event-triage-detecting-system-anomalies/table-of-contents
- Take precautions where possible
  - Solid state drives
  - Limit hardware reuse
  - Monitor for violations of policy including use on unauthorized equipment
- Product manufactures ensure that root privileges are required to modify hardware attributes
- Test for positive detections by modifying and reusing this project's code cyclically

Thank You

References

github.com/arosenmund/blowinghothair/tree/master/references.md

AARON ROSENMUND - PLURALSIGHT

@arosenmund - www.AaronRosenmund.com
www.github.com/arosenmund