



# The Infosec Song Remains The Same

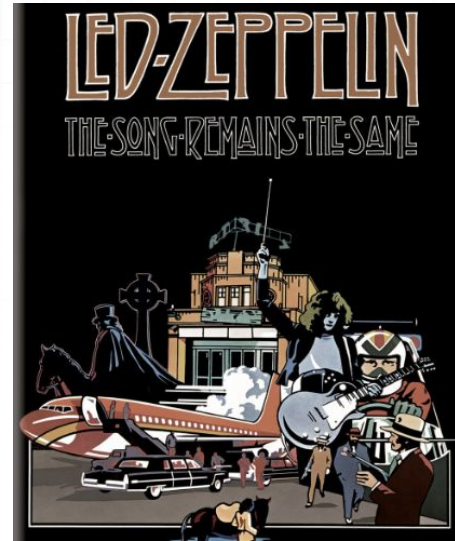
Paul Asadoorian, Principal Security Evangelist, Eclipsium  
<https://securitypodcaster.com>

# What is the meaning of “The Song Remains The Same?”

1. *“how you can travel halfway around the world and people are pretty much the same...”*

**OR**

2. *“the exploitation of Led Zeppelin and how they were a pawn for their label and their management.”*



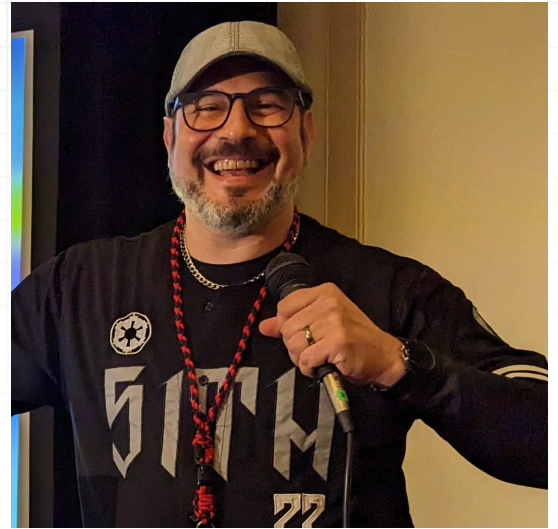
**Throughout our Infosec  
journey challenges  
remain the same.**

# Paul Asadoorian

**Day job:** Principal Security Evangelist for Eclypsiium

**Other job:** Podcast Host for Paul's Security Weekly

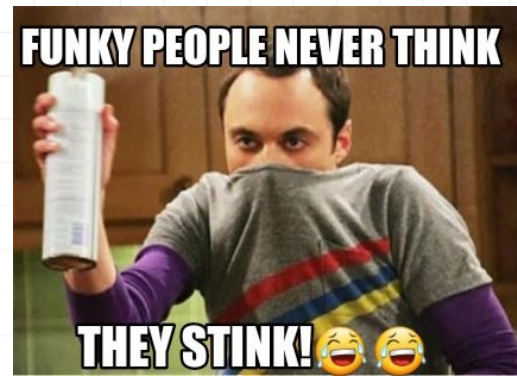
**About me:** <https://securitypodcaster.com>



## Other Noteworthy Things:

*I created a security podcast in 2005, I was employee #98 at Tenable, I've interviewed over 1,000 people in security, delivered over 100 presentations on security, I run Linux as my daily driver, and **I collect memes.***

I've Learned We (Still) Stink At Three Things:

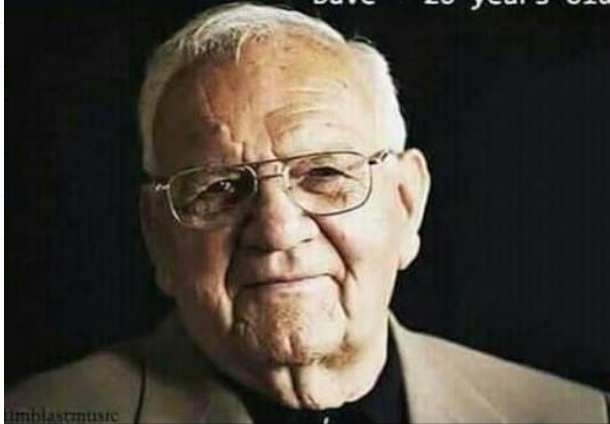


1. **Creating paths to get people into this field**
2. **Properly securing firmware**
3. **Securing the digital supply chain**

**Infosec**

**"Programming is  
not stressful at all"**

Dave - 26 years old



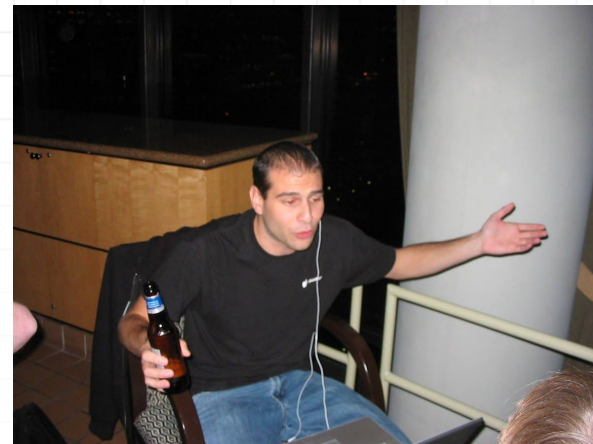
# Getting People Into This Field

# In 2005 I created a podcast

The initial goal was not to encourage people to work in cybersecurity

Rather we wanted to **give back to the community** (and **get together with friends to drink** and talk about security, pretty much in that order)

Amazing fact: So many people have told me **the podcast helped them get into the field** or sparked their interest to work in cybersecurity!



*Larry Pesce was literally there from day 1!*

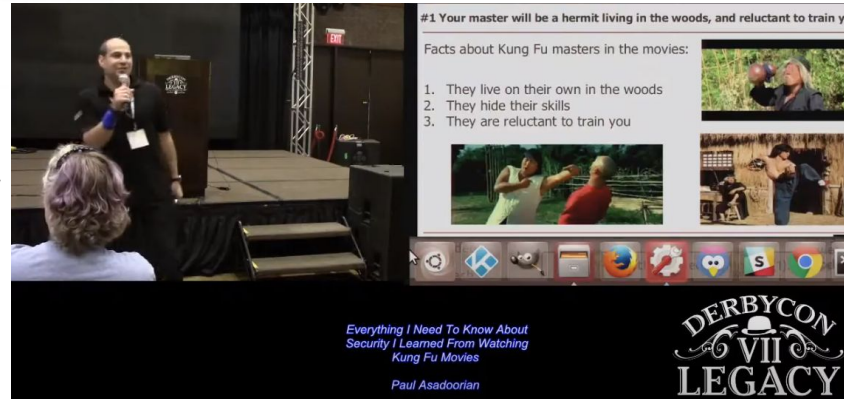


# I Gave A Talk...

**Title:** *"Everything I Need To Know About Security I Learned From Watching Kung Fu Movies"*

**Point:** Kung Fu masters were always reluctant to teach new students.

**Solution:** In our field we need to mentor new students.





# I Gave Another Talk...

## Check The Technique

Go forth and teach in your local community  
(programming, security, hardware hacking, etc...)

Learn how to teach programming, engineering or just general computer topics.

Give classes or seminars in your community for free.

Programming languages are universal and can cross all boundaries.



**Title:** *“Everything Else I Learned About Security I Learned From Hip Hop”*

**Point:** Why aren't there more female rappers | female security professionals?

**Solution:** Teach engineering and cyber security at an earlier age to everyone.

***There is a funny story about my outfit...***



# What's Happening Today?

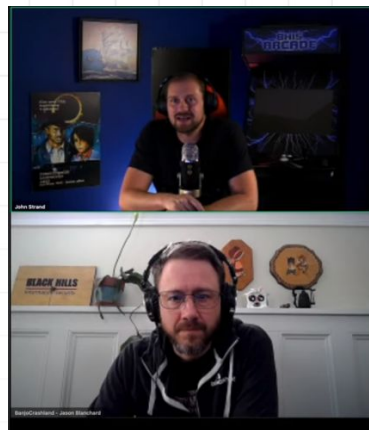
The site I referenced in previous talks, Infosec Mentors, is no longer around

There are some current efforts from John Strand and Tonya Janca and many others (Thank you)

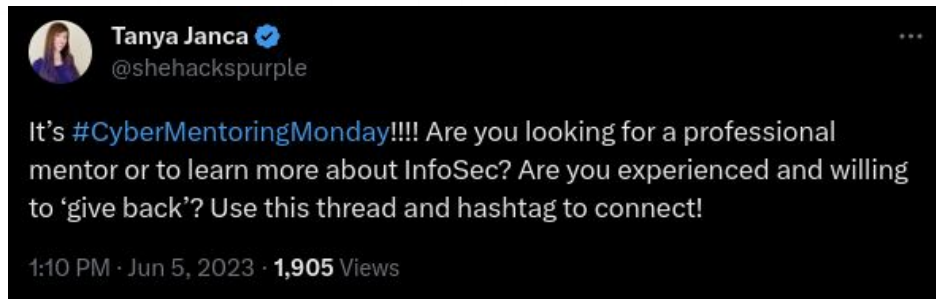
I will also step up:

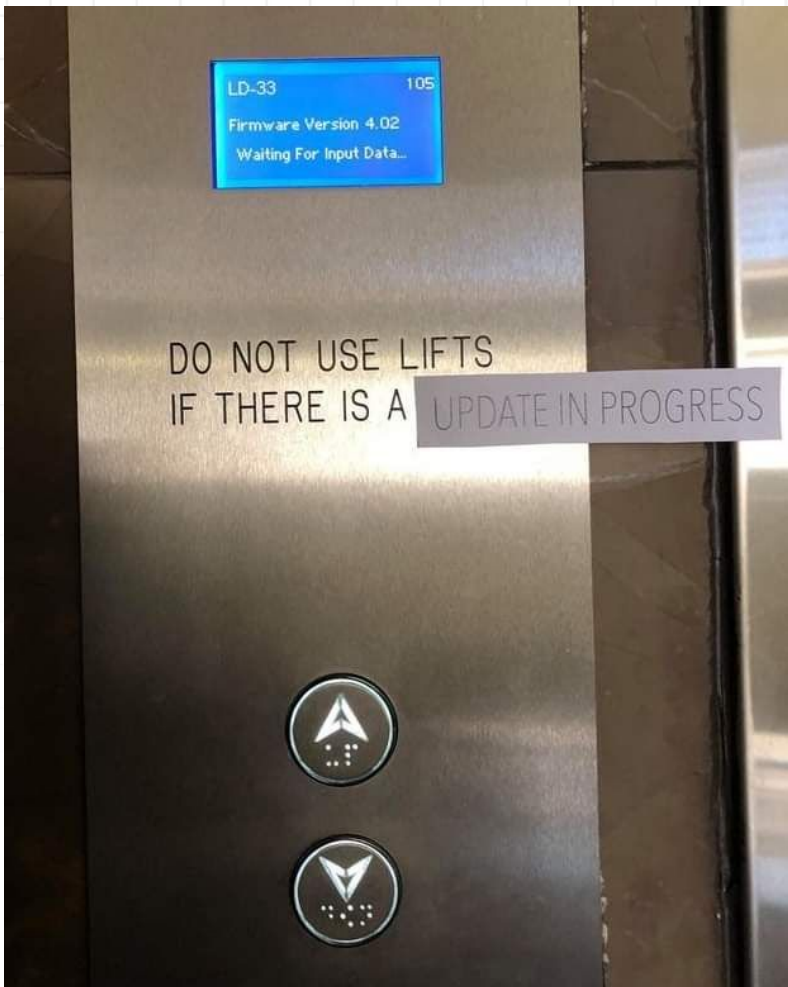
<https://discord.com/invite/pqSwWm4>

Channel: **#mentorship**



[https://www.youtube.com/watch?v=j3\\_xXgNOmQM&t=1488s](https://www.youtube.com/watch?v=j3_xXgNOmQM&t=1488s)





# Properly securing firmware

# Firmware - Still Hacking Like It's 1999

In 2010 at Brucon I presented "Embedded Systems Hacking and My Plot To Take Over The World"

This was before Mirai

The premise: How and why do attackers use what we now call IoT devices?

My monetization methods were not a great prediction

## Using Embedded Systems To Make Money

- **Video games** - Most are involved in commerce and network connected
- **Entertainment** - Apple TV, Roku, all link back to your credit card somehow
- **Wireless routers** - Route your traffic when doing online banking, Paypal, Ebay, etc...
- **Printers/Fax** - How many times have you printed sensitive information?



# The 10 Most Wanted List

NOLAcon 2014 I presented:

## The Internet Of Evil Things: The 10 Most Wanted List

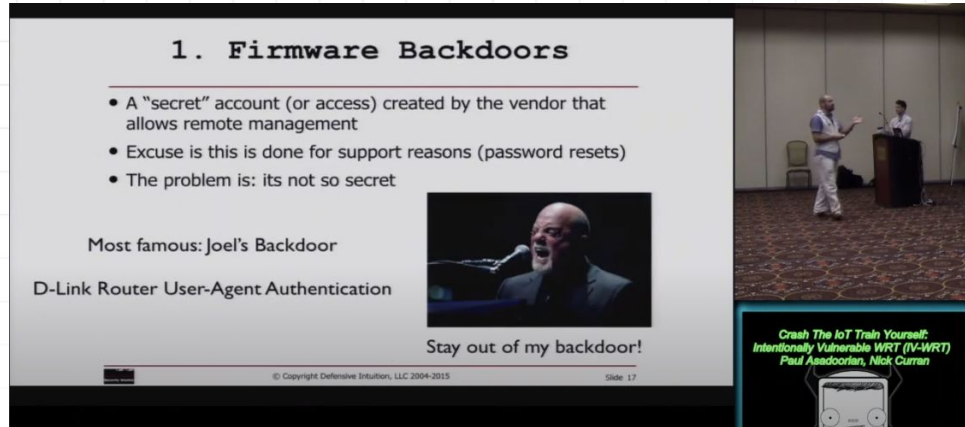
We still see all of these issues today...

## 10 Most Wanted List

---

1. Backdoors inside of firmware
2. Default credentials
3. Insecure Remote management (Defaults & Clear-Text Transmissions)
4. Open-source software and drivers, NOT **binary blobs**
5. Functions prone to overflow conditions
6. Firmware and configuration encryption
7. Easy-to-use firmware updates (auto-updates)
8. Secure web management interfaces
9. Maintain a CIRT and provide a program for security researchers
10. Implement Protocols Security / Implement Secure Protocols

# The Intentionally Vulnerable Effort



**1. Firmware Backdoors**

- A "secret" account (or access) created by the vendor that allows remote management
- Excuse is this is done for support reasons (password resets)
- The problem is: its not so secret

Most famous: Joel's Backdoor

D-Link Router User-Agent Authentication

Stay out of my backdoor!

© Copyright Defensive Intuition, LLC 2004-2015 Slide 17

*Crash The IoT Train Yourself: Intentionally Vulnerable WRT (IV-WRT) Paul Asadoorian, Nick Curran*

At BSidesLV 2015 I co-presented with Nick Curran at talk titled: Crash The IoT Train Yourself: Intentionally Vulnerable WRT (IV-WRT)

We released a vulnerable on purpose firmware distro based on OpenWRT.

It was fun, but did not garner much attention.

See Saumil's project for the modern day version of this:  
<https://github.com/therealsaumil/emux>

# I Gave Up On Firmware (For A While)

I left Tenable to run Security Weekly full-time

I focused on the podcast business and developing software to automate podcast production

Until 2017...

Another juggler gives up on his dreams...



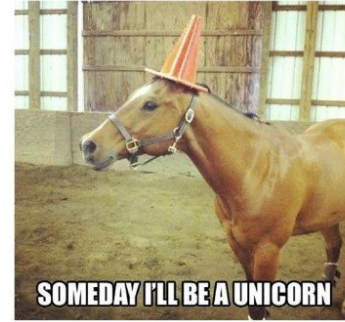


# I Gave A “Crap is still vulnerable talk” Again...

## I Gave Up

After years on the subject, I gave up

IoT devices were more ubiquitous, and just as vulnerable as ever



Source Boston Conference 2017 I gave a talk titled: “IoT Security: My Worst Nightmares Come True and How To Sleep Better At Night”

Firmware was still being attacked, Mirai was released

Glimmers of hope were the FDA started taking notice, The FTC issued some fines, grants were issued and CyberUL was a thing

Then, **I gave up again and worked on various other projects**, Security Weekly was acquired in 2020...

## But Then In 2022 - A New Hope?



*You must come with me to work on firmware again...*

I had an opportunity: Pursue a new journey in cyber security

What is still broken? - Turns out...Firmware!

Some really smart people were telling me that PCs, servers, and laptops all contain copious amounts of firmware, and there was no shortage of vulnerabilities

I began researching the topic, and quickly learned that I had much to learn...

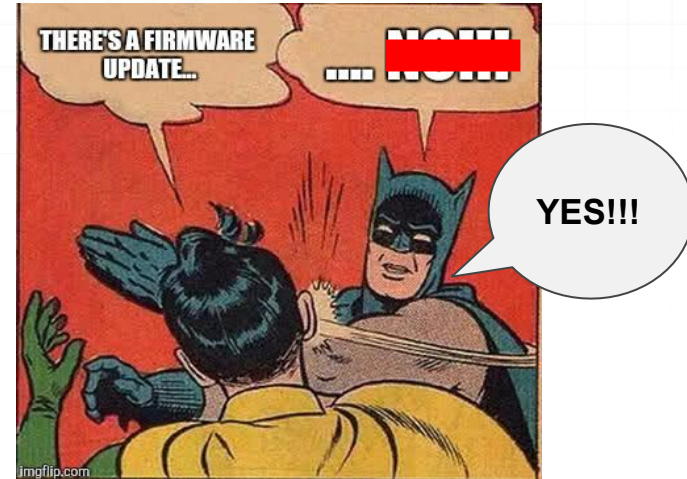
# Firmware Realizations

*Firmware is just software that is inconvenient to program*

There is an unspeakable amount of “things” that happen (with firmware) from when you press the **power button to when you are presented with a login screen**

Firmware still contains **the same problems I was talking about 10+ years ago**

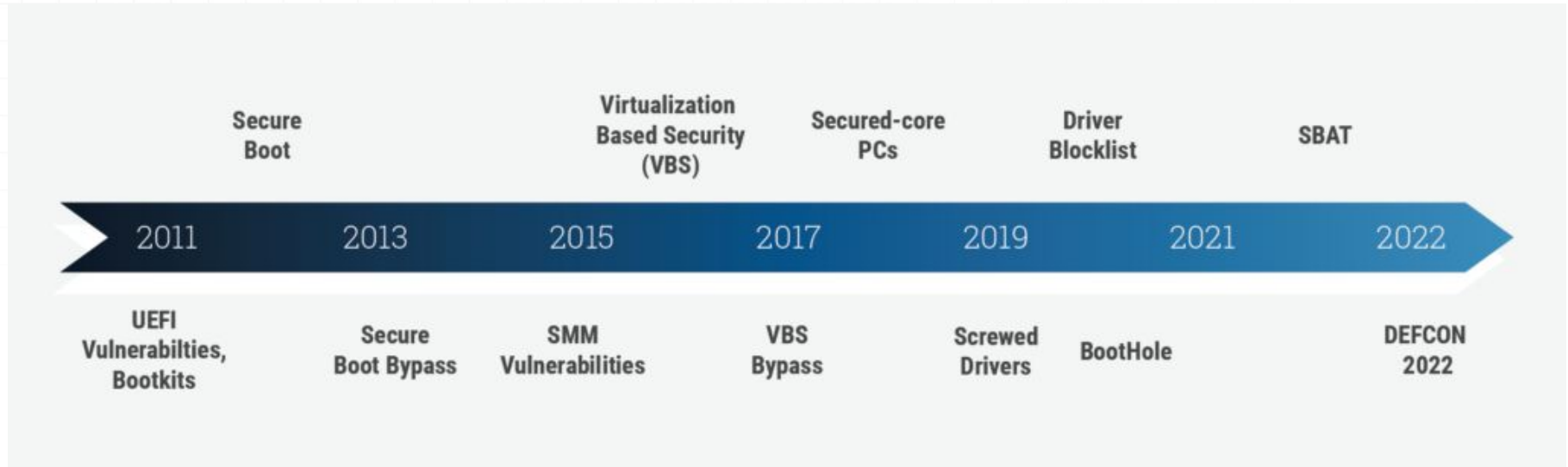
Firmware still lives **below the surface**, people expect it to just work and are hesitant to update it





# A Brief History Of How Iron Sharpens Iron In Firmware Security

<https://eclypsiium.com/blog/a-brief-history-of-how-iron-sharpens-iron-in-firmware-security/>





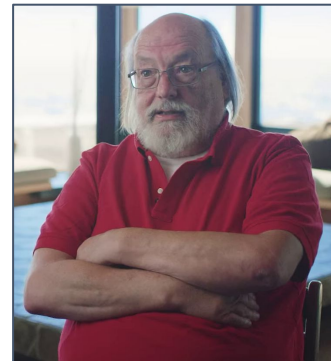
**Ruth Buchanan**    
@RuthMBuchanan

From now on when people ask why I'm not married, I'll just say it's a supply chain issue.

# Securing the digital supply chain

***“You can't trust code that you did not totally create yourself.”***

***“No amount of source-level verification or scrutiny will protect you from using untrusted code.”***



“Reflections on Trusting Trust” - Ken Thompson, August 1984, Volume 27 Number 8,  
Communications of the ACM

[https://www.cs.cmu.edu/~rdriley/487/papers/Thompson\\_1984\\_ReflectionsonTrustingTrust.pdf](https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf)

# A Matter Of Trust: How can we trust what we can't see?



**Applications**

**Operating Systems**



**UEFI/BIOS & Other  
Firmware**



# The Digital Supply Chain Attack Surface

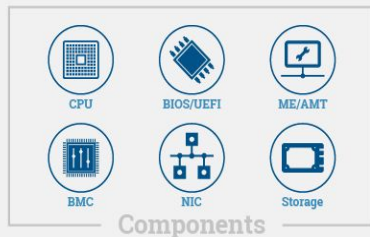
Reduced Visibility = Validation Challenges

## PHYSICAL



“Hunting for backdoors in Counterfeit Cisco devices”

## PRE-INSTALLED



Components

Firmware

Bootloaders

Kernels

Operating Systems

## 3RD-PARTY APPLICATIONS

slack zoom

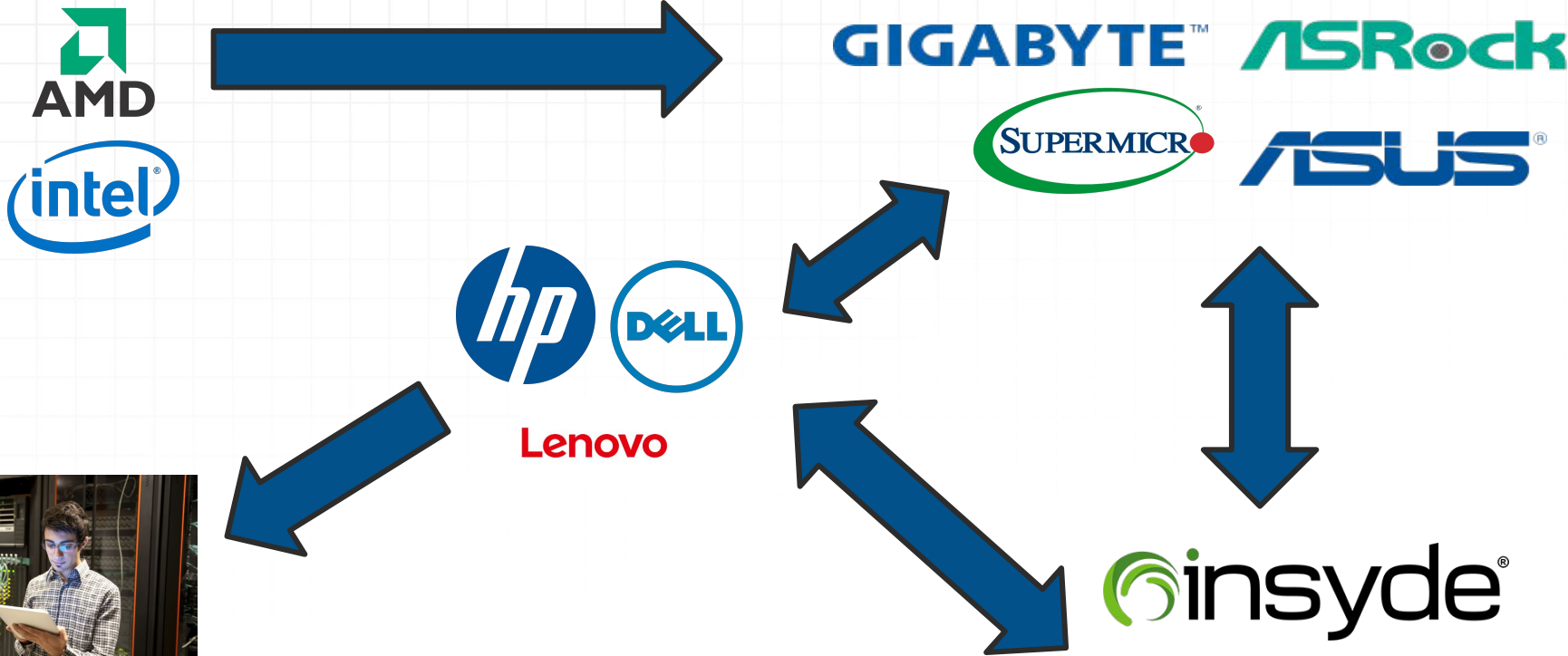


## SOFTWARE DEVELOPED IN-HOUSE



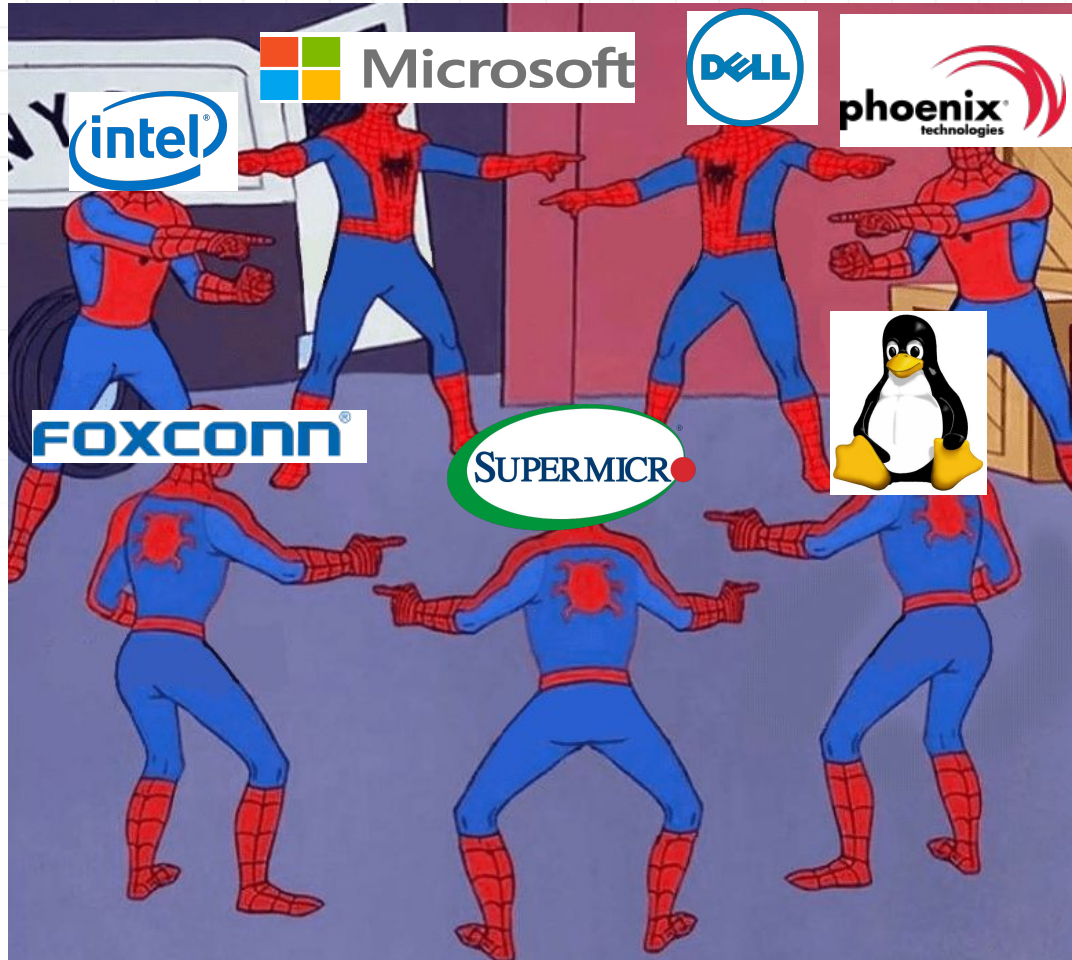
Increased Customization & Control

# The Supply Chain for PCs, Servers, and Laptops



Consumers/IT Dept.

# Who Fixes It?



# How do we minimize supply chain risks?

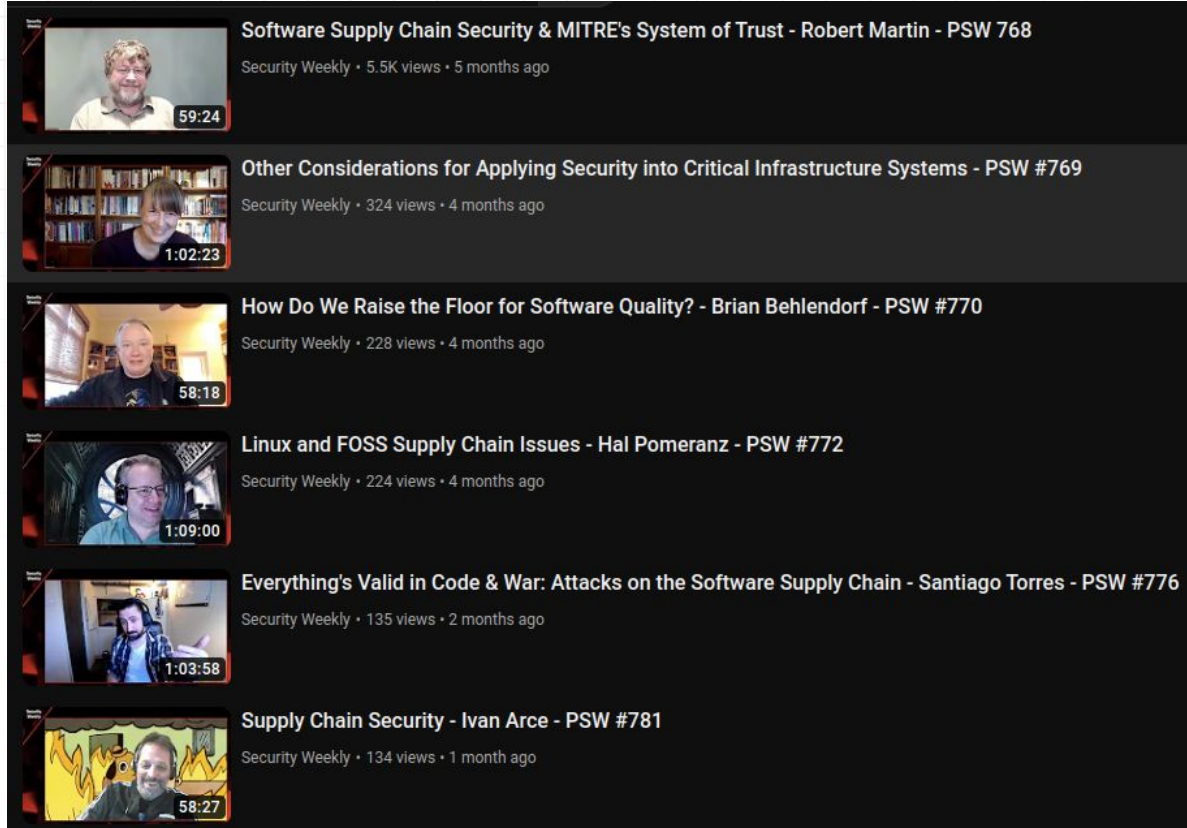


**Create  
everything  
myself**

**Verify, then trust.  
Make attackers  
lives more  
difficult.**

**Create nothing  
and do no  
verification**

# Supply Chain Interviews - PSW & BTS

A vertical stack of six YouTube video thumbnails. Each thumbnail shows a video player with a speaker icon, a video frame, a title, and view/viewer information. The video frames show different people in various settings, including a man in a white shirt, a woman in a dark top, a man in a dark jacket, a man in a light blue shirt, a man in a plaid shirt, and a man in a dark jacket with a cartoon overlay.

**Software Supply Chain Security & MITRE's System of Trust - Robert Martin - PSW 768**  
Security Weekly · 5.5K views · 5 months ago  
59:24

**Other Considerations for Applying Security into Critical Infrastructure Systems - PSW #769**  
Security Weekly · 324 views · 4 months ago  
1:02:23

**How Do We Raise the Floor for Software Quality? - Brian Behlendorf - PSW #770**  
Security Weekly · 228 views · 4 months ago  
58:18

**Linux and FOSS Supply Chain Issues - Hal Pomeranz - PSW #772**  
Security Weekly · 224 views · 4 months ago  
1:09:00

**Everything's Valid in Code & War: Attacks on the Software Supply Chain - Santiago Torres - PSW #776**  
Security Weekly · 135 views · 2 months ago  
1:03:58

**Supply Chain Security - Ivan Arce - PSW #781**  
Security Weekly · 134 views · 1 month ago  
58:27



# We've Had Some Major Wins

- **March 2023** – the FDA issued a guidance for immediate implementation: Cybersecurity in Medical Devices: Refuse to Accept Policy for Cyber Devices Under Section 524B of the FD&C Act [1].
- **December 2022** - NIST published [Validating the Integrity of Computing Devices \(1800-34\)](#) - A guide on how to validate the supply chain including examples using major OEMs such as Dell and HP.

This is what winning looks like..😎



# We've Had Some Major Wins

- **September 2022** - [Executive Order \(EO\) 14028](#) directs NIST to issue guidance “identifying practices that enhance the security of the software supply chain.” and directs the Office of Management and Budget (OMB) to require agencies to comply with such guidelines (including firmware).
- **August 2019** - France defines hardware and firmware requirements for IT systems [2].





## In Conclusion

- Be involved in mentoring (and join our Discord channel if you like)
- Firmware is still broken, we need people at both technical and policy levels to help fix it
- In order to trust the digital supply chain we need everyone to play a role in verifying each component
  - Attestation
  - Cryptographic verification
  - Checks and balances

The Institute of  
Unfinished Research  
has concluded that  
6 out of 10 people

# Thank You!

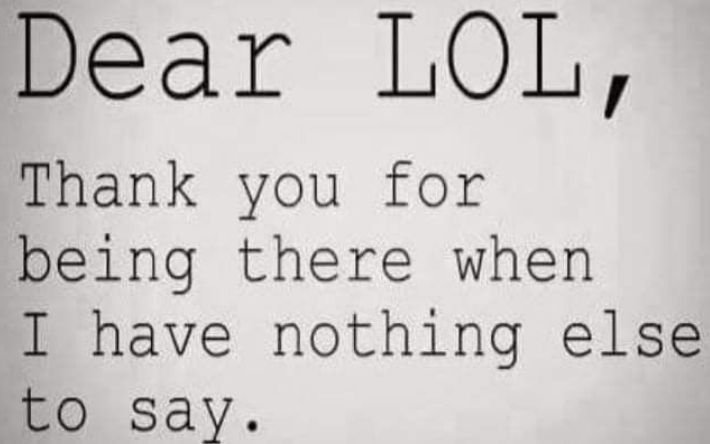
Presentations referenced in this presentation are here:

<https://securitypodcaster.com/presentations/>

Contact me: <https://securitypodcaster.com/contact/>

Subscribe to my podcasts:

<https://securitypodcaster.com/podcasts/>

A photograph of a piece of paper with a typewriter-style message. The text is in a monospaced font and reads: "Dear LOL,  
Thank you for  
being there when  
I have nothing else  
to say." The paper is slightly off-white and the background is dark.

Dear LOL,  
Thank you for  
being there when  
I have nothing else  
to say.