Wingin' It

On-Wing Pentesting And Why You Should Do It

Or

Some Cool Hacker Stuff We Did On A Plane

Or

How I Hacked a Plane and Didn’t Get the Feds Involved

I couldn’t pick a title…

Who the heck is this goofball?

@elder

Alexander Dodd

- Attack Research –
  Security Consultant/Researcher/Penetration Tester
- USAF Veteran
- Too boring for social media but sometimes @attackresearch
- Absolute Goon
- Cyber Idiot #J

https://www.attackresearch.com/

#Goals

Airline Folks

- Show you why this is important
- How can you get it done safely

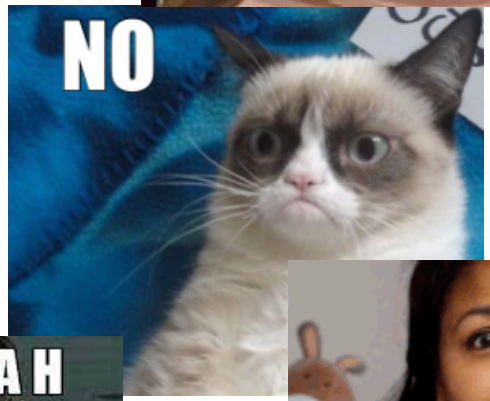
Hacker Folks

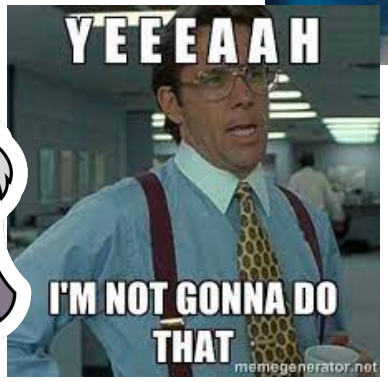
- Dudes, there's some goofy stuff
- Hacking physical things is dope

** I'm not an aviation expert or authority.

Things I'm NOT going to do

- Divulge the airline
- Tell you how to destroy or take over avionics





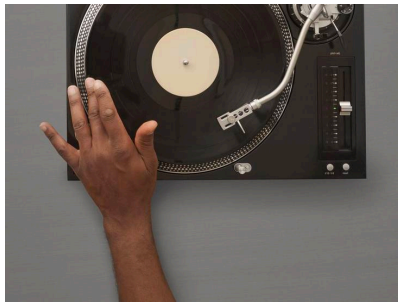
Why Do You Care? (Airline Folks)

- There's no substitute for getting hands on actual equipment.
  - Manufacturers claim they're testing, but are sometimes unable/unwilling to share test results/information
  - Do you inherently trust your third-party webapp library developers or do you still add "the website" to your pentest scoping?

- "Newer" doesn't necessarily mean "Better"
  - We'll talk a bit about the differences between the 737NG and newer platforms

Why Do You Care (Hacker Folks)

- There's no substitute for getting *your* hands on actual equipment.



You're probably wondering how I ended up in this situation...

- We do a lot of work in the airline In-Flight Entertainment (IFE) and Payment Processing (PCI) industries, so we have some friends around.
- Last year we were asked if we wanted to come hack a plane that was **en route to be decommissioned**. Don't @ me about it.
- I'm pretty sure the bosses only said yes to this because they knew we were going to riot like French firefighters if they didn't.

WE ALREADY REPORTED TO THE AIRLINE.
Please don't yell at me about responsible disclosure and/or security leaks.

Team/Company Goals

- Do a Business(?)
- Training and Experience for the gang
- Don’t let Dodd injure himself with a drill

Personal Goals

- Find a way to cause Panic on a plane
- Tamper the hell outa some smoke detectors
- Learn some new stuff

What We Knew Going In

The target aircraft was a Boeing 737NG (Next Generation) which, according to Wikipedia, was in production from around 1996 to 2019.

Some of our team has tested on a 737MAX as well as parts for the 777 and 787 in the past. This was hopefully going to be similar.

What We Didn't Know

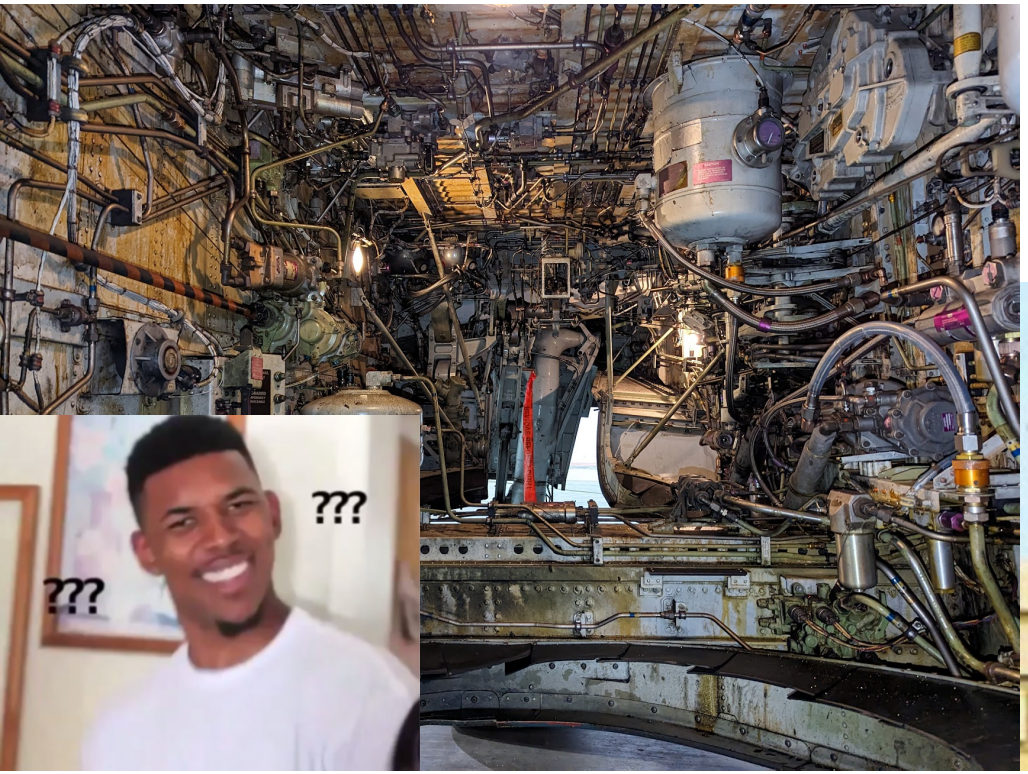
Good luck Googling;

"How to hack a plane"

"Hacking plane, where start?"

"737 avionics controls remote takeover"

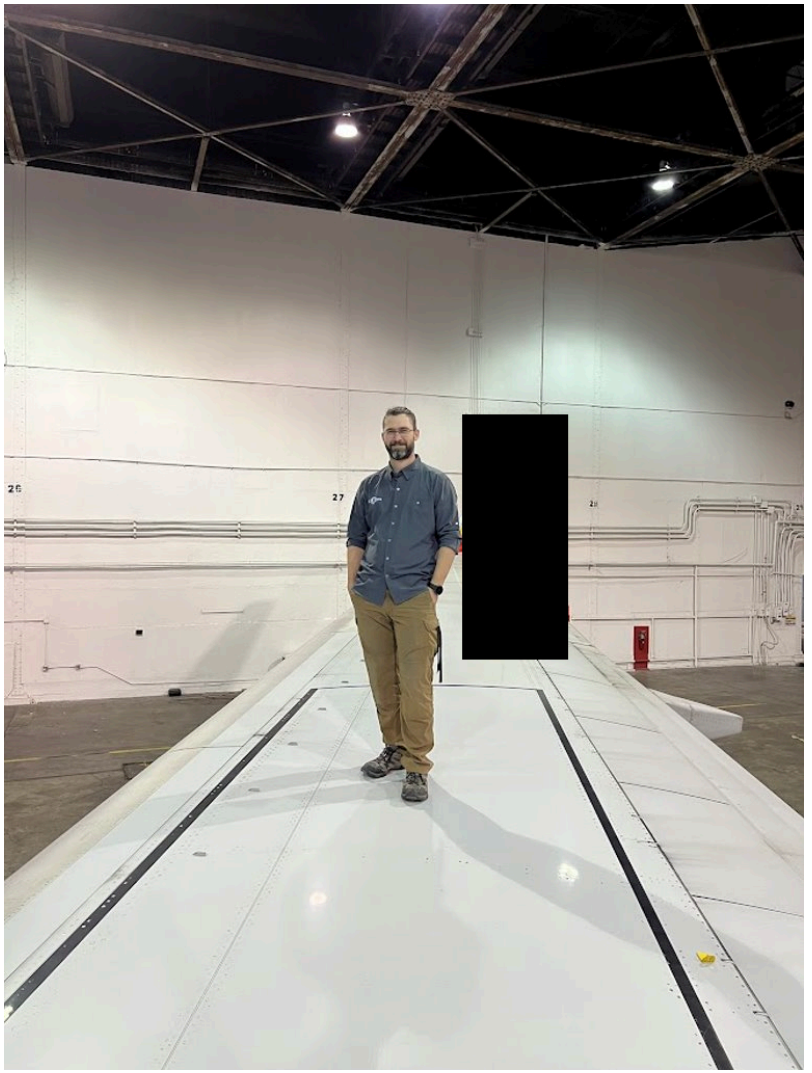
"Alphabet Soup Van at my house why?"



I'mma be real with you… Basically everything on this machine was new to me. Contrary to popular belief, having been in the Air *Force* for nearly a decade does *not* mean one knows anything about Air *Planes*.

Not our standard testing environment

It's not often we do our work in a freezing cold hangar. Anything we needed was going to have to be brought or bought.



Phase 1 - Site Survey and Begin Goonery

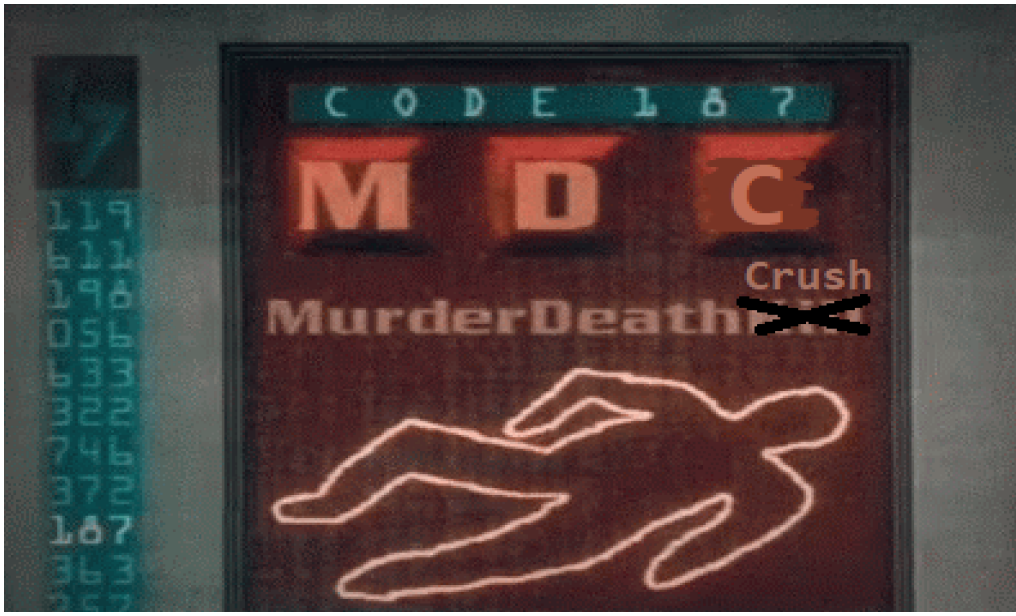
- Are there tools we can use?
- What are the ROEs?
- Who is in charge around here?
- Tear panels off everything and look for ports.
- Can I open the emergency exit for fun?
- Does it look like I can scramble on TOP of the plane before anyone notices?
- Follow-up question; How hard is that floor?

Safety Third

Beer, Style, Safety in that order

Limitations set by client

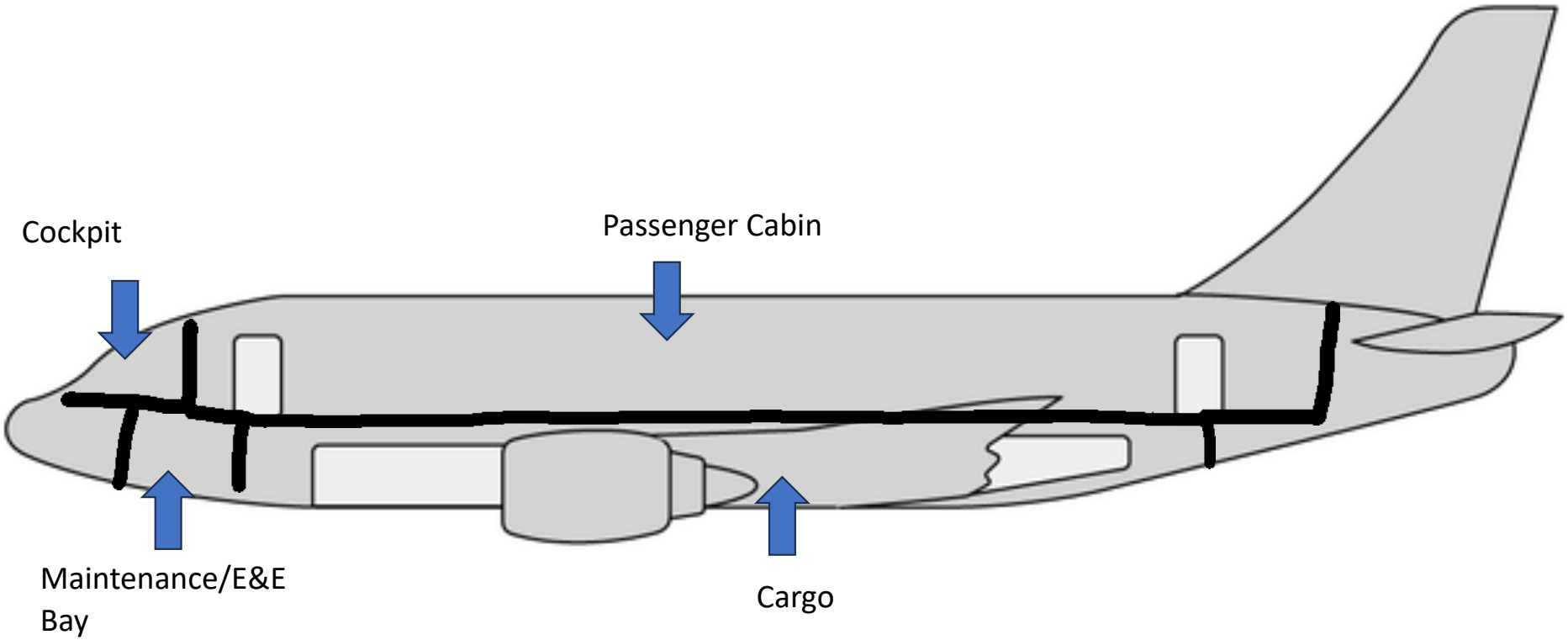
Don't touch the engines.
Don’t break the LRUs.
Do Not Touch the landing gear lever thingy… for safety



Limitations inherent to the environment

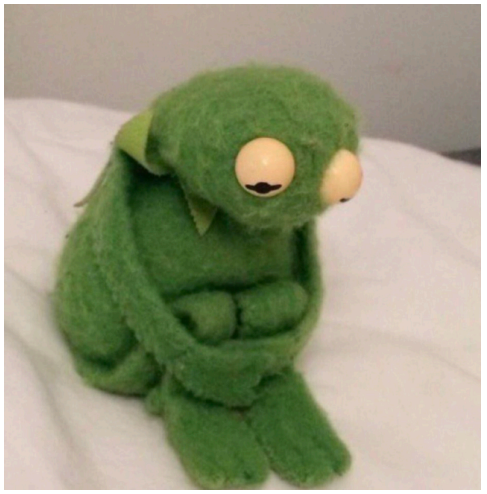
Cell signal in the hangar was next to nil. Cell signal inside the cabin was nil. Satellite connection to provide inflight WiFi was unavailable (see previous statements re: being inside a hangar).

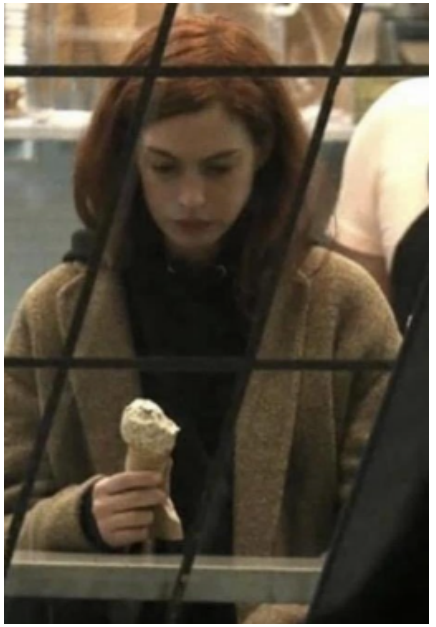
Super Professional and Precise Diagram



-> Cockpit

There was another team there doing similar testing. They had dibs on the cockpit. :(





-> Maintenance Bay / LRUs

This little box was Cramped™

We had to share it with the other goobers, so our time in the AdSeg was limited, but we did hook into all the Ethernet and serial ports to see if there was anything interesting happening.

LRUs Control;

- Air/Ground Communications
- Air/Air Comms
- TCAS - Traffic Collision Avoidance System
- DFDAU – Digital Flight Data Acquisitions Unit
- FADEC – Full Authority Digital Engine Control
- In-Flight Entertainment System(s)
- "Other Stuff"

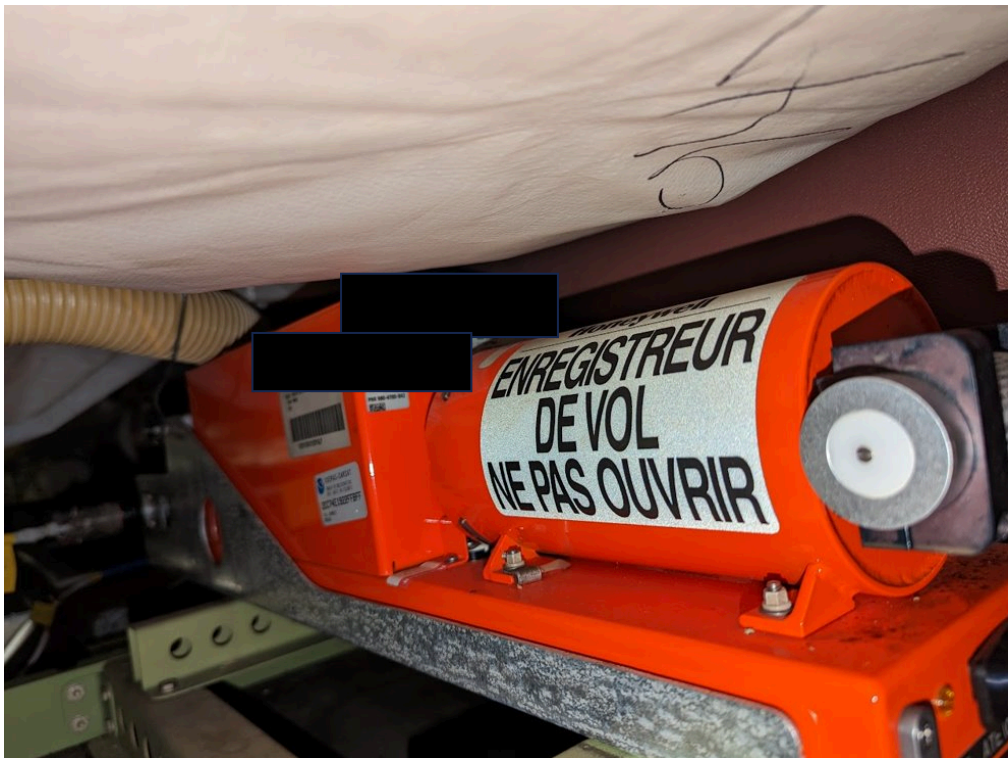
-> Cargo Bay


BHD
727+4

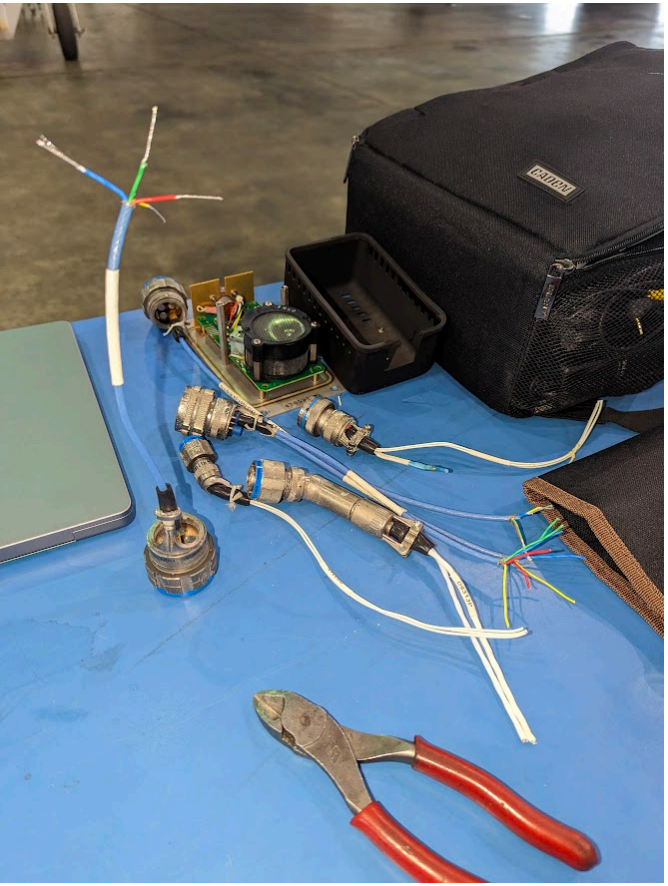

4 Bonus Imaginary Hackerpoints if you know what's behind this panel

The Lavatory Tank

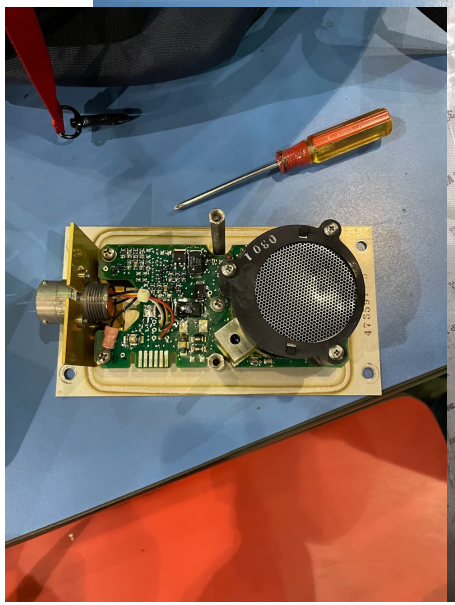
The Black* Box*



Smoke Detectors



Federal law prohibits tampering with, disabling, or destroying any smoke detector in an airplane lavatory.



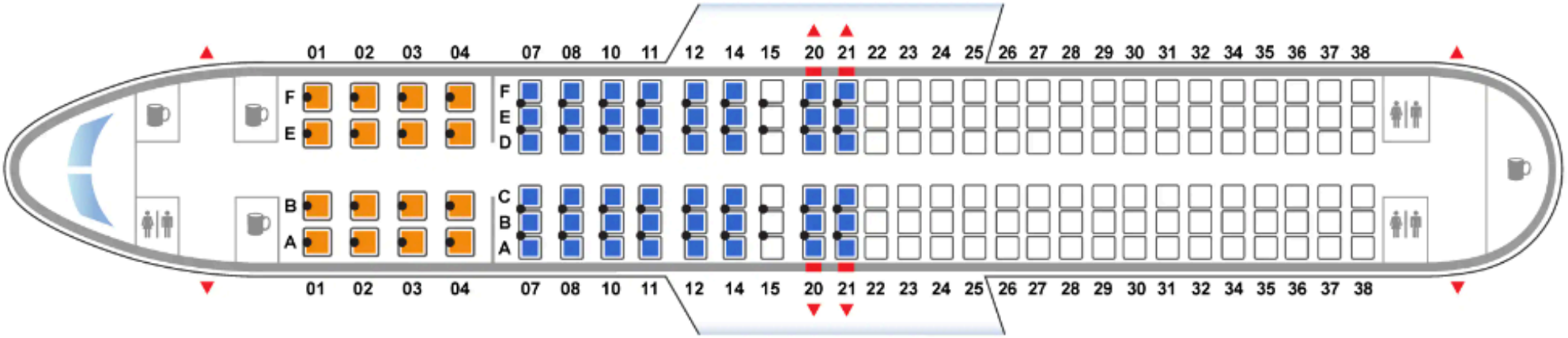
ARINC 429 and 615

**Shamelessly stolen from Wikipedia. Donate your $3, folks.

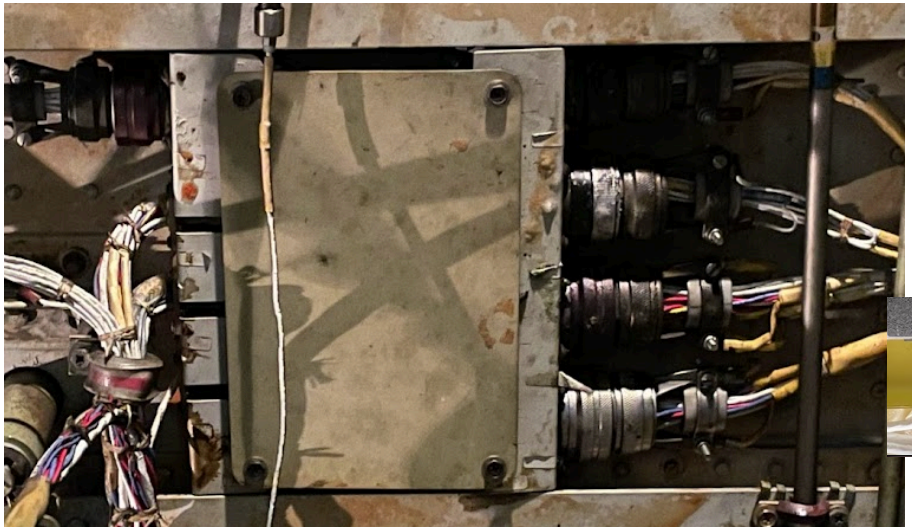
ARINC 429 is a data transfer standard for aircraft avionics. It uses a self-clocking, self-synchronizing data bus protocol (Tx and Rx are on separate ports). The physical connection wires are twisted pairs carrying balanced differential signaling. Data words are 32 bits in length and most messages consist of a single data word. Messages are transmitted at either 12.5 or 100 kbit/s[3] to other system elements that are monitoring the bus messages. The transmitter constantly transmits either 32-bit data words or the NULL state (0 Volts). A single wire pair is limited to one transmitter and no more than 20 receivers. The protocol allows for self-clocking at the receiver end, thus eliminating the need to transmit clocking data. ARINC 429 is an alternative to MIL-STD-1553.

ARINC 615A is a standard that covers a "data loading" protocol which can be used over various bus types such as Ethernet, CAN, and ARINC 664.

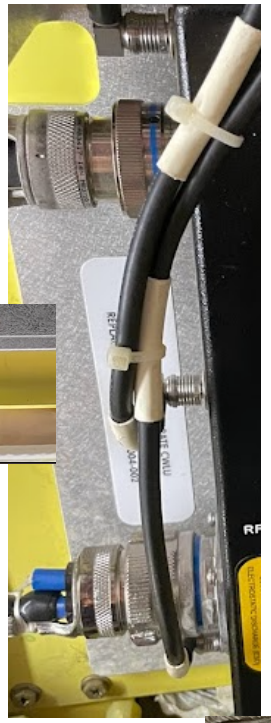
-> Passenger Cabin

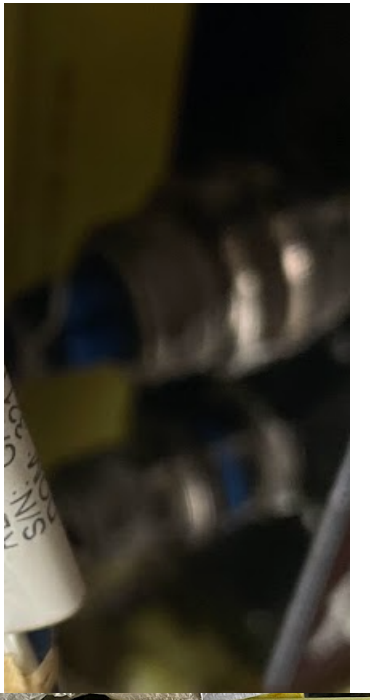


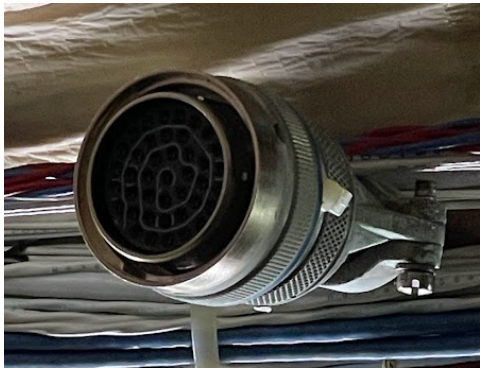
** I don't have any pictures I can show you from inside the cabin. Y'all know what the inside of a plane looks like...

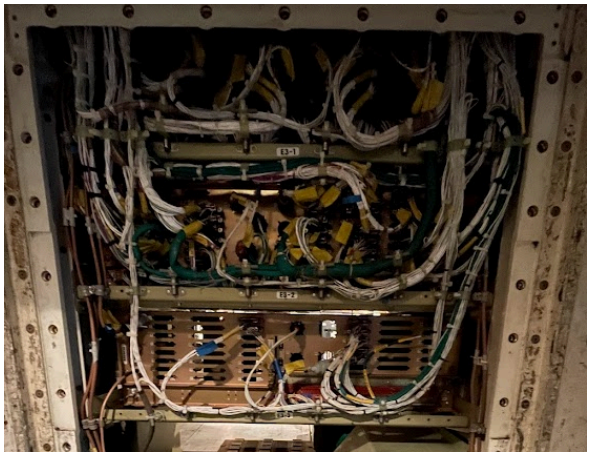


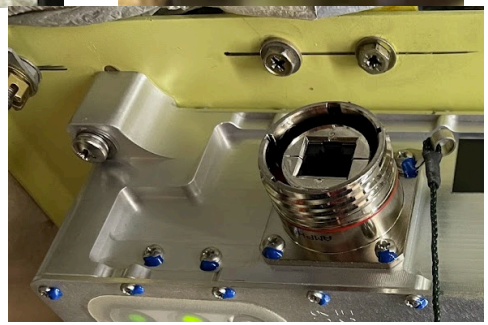

J7
J6



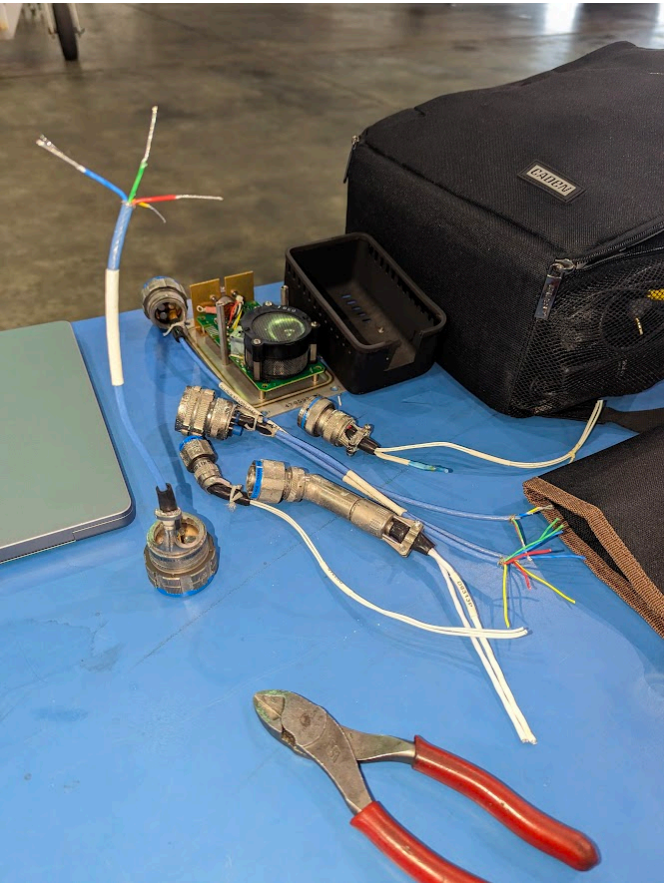


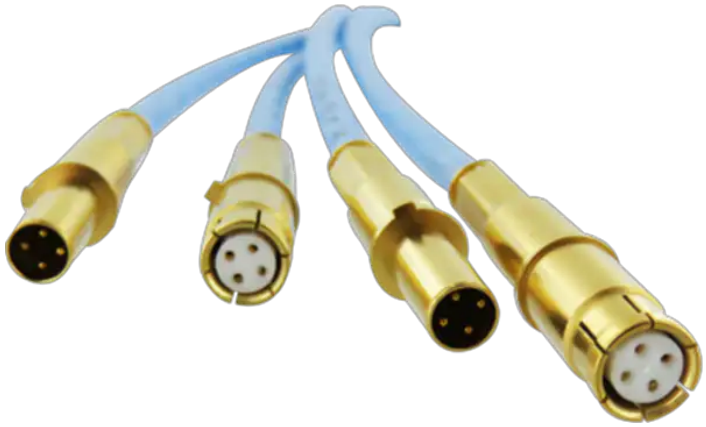






Quadrax





Quadrax Pin with 8P8C “RJ45” Jack

Why?

1) RJ45 connectors are just bad.

2) Weight

Smaller and lighter than using a full four-pair CAT5 for systems that don't require the higher speeds. Half as much copper weight plus a sturdier connection instead of plastic with little breakable tangs that call your name like that clip on a mechanical pencil.

Threeory) It's just a better cable solution for this application.

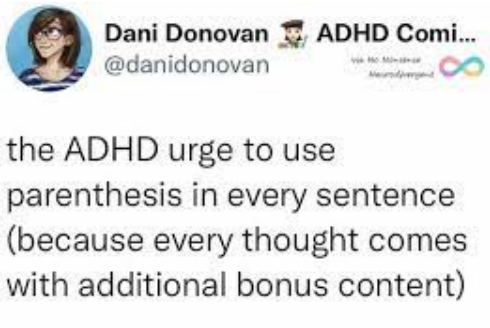
Dear Diary, Day Three - Begin Scan and Bang

Assign ourselves an IP, nmap, tcpdump/wireshark, nikto, gobuster, try some sloppy ssh and telnet… you know… do hacker stuff.

Series of 10.x.0.0/24 networks.

We seem to be between passenger and crew networks. Satellite modems, Cell modems, and other non-passenger-friendly systems are stashed back here.

Sidebar - Kinda



Default credentials were a **plague** on this network. admin/admin and admin/password were masterkeying us in to just about everything.

- Cell and Satellite modems
- Switches
- WAPs

```
Login incorrect
          login: admin
admin
Password: admin

1 ansi
2 gnome
3 kterm
4 vt100
5 vt102
6 vt220
7 xterm
Enter 1..7 to choose terminal type, q to quit: q
q
alex@Alexanders-MacBook-Pro wordlists % nc 10.2.0.1 23
```

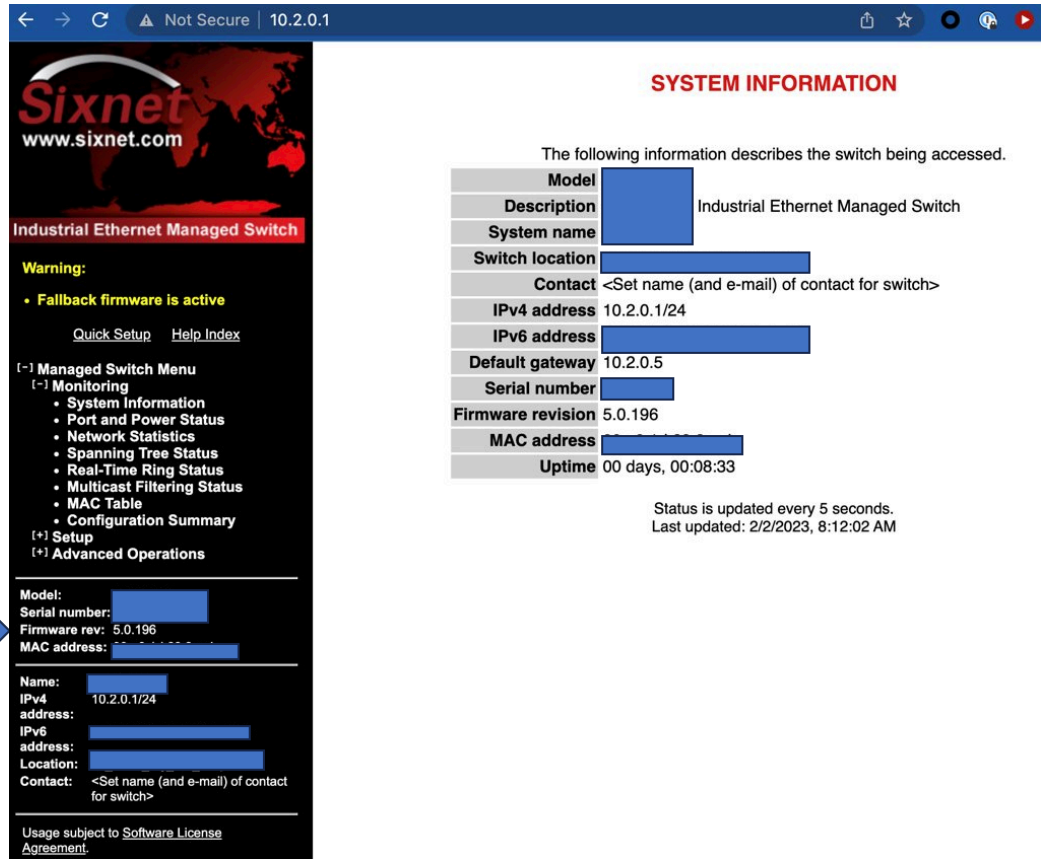
Sidebar to the Sidebar…

These things were old. DOS old. This incidentally made things More difficult. It's one thing to look at Wordpress 3.x or VSFTPD 2.3.4 or WinXP with RPC and chuckle, but we didn't have any exploits or implants on deck for anything that old. Security Through Obsolescence?

We took down the network… Oops.

Identify the enabled switchports, mirror them all to where we're connected, sniff for traffic… and we bottomed out. Recursion is a helluva drug.

This firmware version is from 2012.



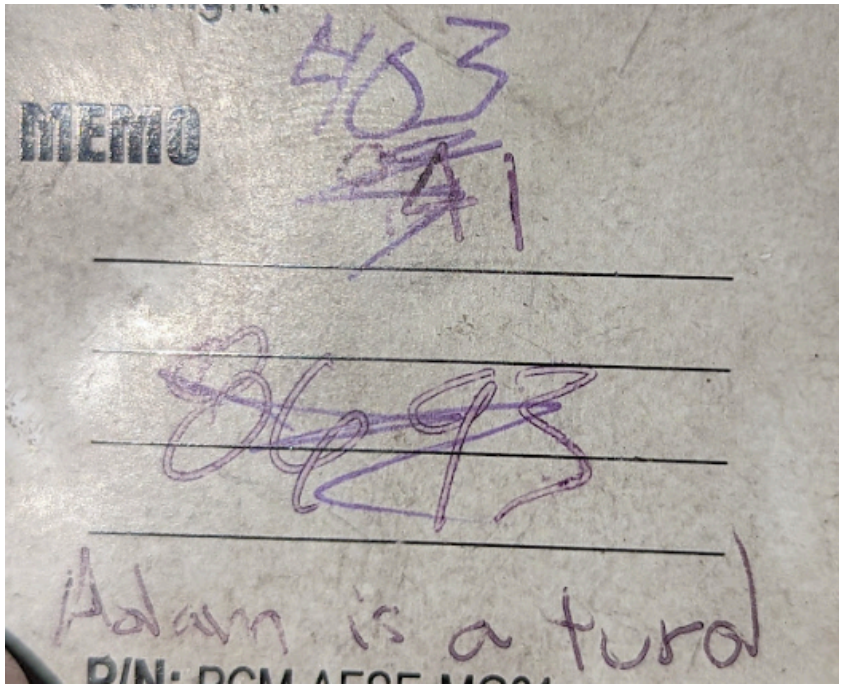
Massive Attack Surface Upgrade* NG vs. MAX

*for attackers

- Some components of the MAX can accept commands via text message
- More and easily accessible RJ45s
- According to MX PAX - Much of the NG maintenance tasks are done by maintenance personnel from the physical part while MAX allows remote(ish) triggering of tasks from the maintenance laptop. This can cause damage if not in the proper configuration. This converts the MX laptop into an extension of the attack surface for the plane.

Not What I Mean by "Part Signing"

- Part Signing is handled in a new way;
  - NG - Parts provided by avionics manufacturer [Boeing, Raytheon, Teledyne, etc]. Manufacturer may or may not sign package.
  - MAX – Airline/Owner is responsible for signing packages. This adds another attack surface (entire backend infrastructure for signing packages)



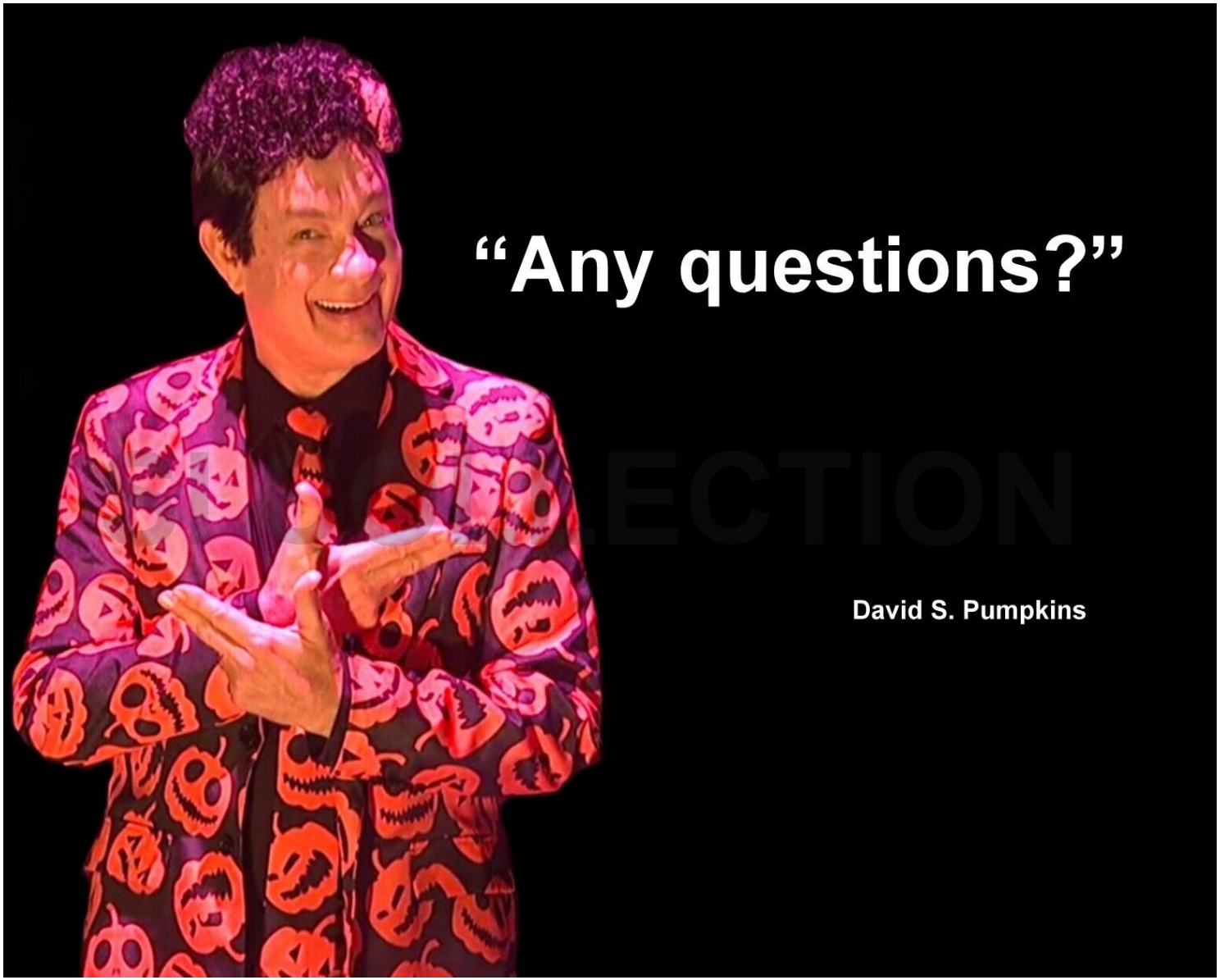
*All the dudes named Adam I know are actually alright...

Why is this guy still up there?

- My role here is not to cause panic.
- Understand attack surface so it can be better defended.
- Not here to attack airlines, OEMs, or manufacturers.
- Whether buying a network switch or a 737, your hardware vendors likely didn't secure their systems for *your* network configuration. Review the settings and ensure they’re up to snuff. They have configuration pages for a reason.

Sources

- https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm
- https://skybrary.aero/
- http://www.b737.org.uk/
- We did a thing and I took some pictures.
  - There was like an official report and everything.


“Any questions?”
David S. Pumpkins