Vulnerability disclosure in Aviation

How it should not be done!

- Matt Gaffney – a.k.a Gaffers
- Aerospace Village DEF CON 33
- @CyberGaffers

Vulnerability Disclosure in Aviation

- **Real-world examples**
  - **Good, Bad, and Ugly**
- **Dos and don’ts**
  - **Researchers**
  - **Recipients**

Gaffers

Hacker – Veteran – Aviation nerd

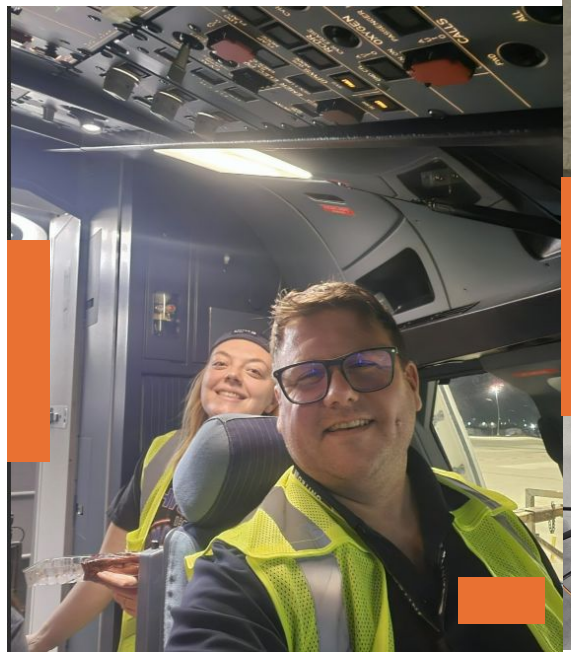
Previously: British Army, UK FCO, various French companies

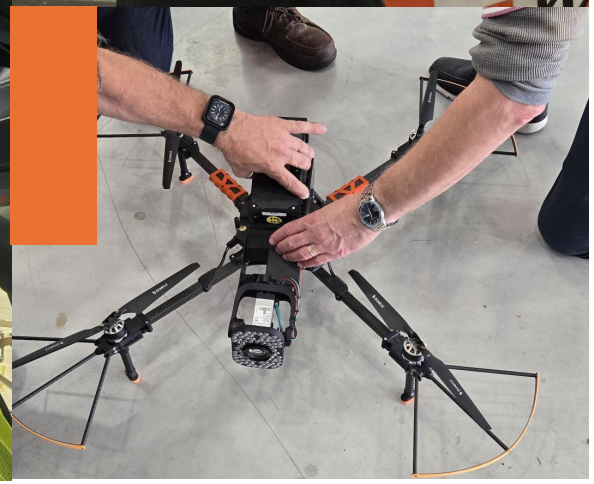
Working in aviation since 2016



‘Forced’ into research!

- EFBs
- PKI
- UAS
- Website auth vulns
- CVEs for Java and more!
- Social Engineering





Personal experiences

Code vulnerability in EFB software discovered during a PenTest:

- Investigated further post-test gathering pilot and SME input
- Potential impacts to Safety were identified
- Initial disclosure to supplier met with “Not a vulnerability, but a feature”
- Over 9 months of challenging discourse, including discussions with regulators
- A several year action plan was agreed.
- *Pandemic and a change of employer*
- On follow-up 5 years later “You’re no longer our client, we won’t discuss anything with you. Oh, and our code is IP”

Issue relating to operator compliance with ICAs (Instructions for Continued Airworthiness):

- Wrote up and sent directly to known contacts (existing relationships)
- Multiple back-and-forth to discuss and explain
- Collaborative work sessions to figure out how to implement the correct method
- Documented for others to follow suit
- Agreed change to ICAs and timeline for distribution
- Kept the regulator informed all the way through

Village experience

Talk submission from researchers discussing a vulnerability:

- Told us the VDP process was complete
- Due diligence by the Village with manufacturer “No, it’s not complete! You cannot talk about this at DEF CON!”
- Researchers dropped the receipts showing responsible disclosure and taking it through to ‘closure’
- Manufacturer ‘accepted’ the risk without making a change
- Failed to negotiate with the researchers about holding back public disclosure

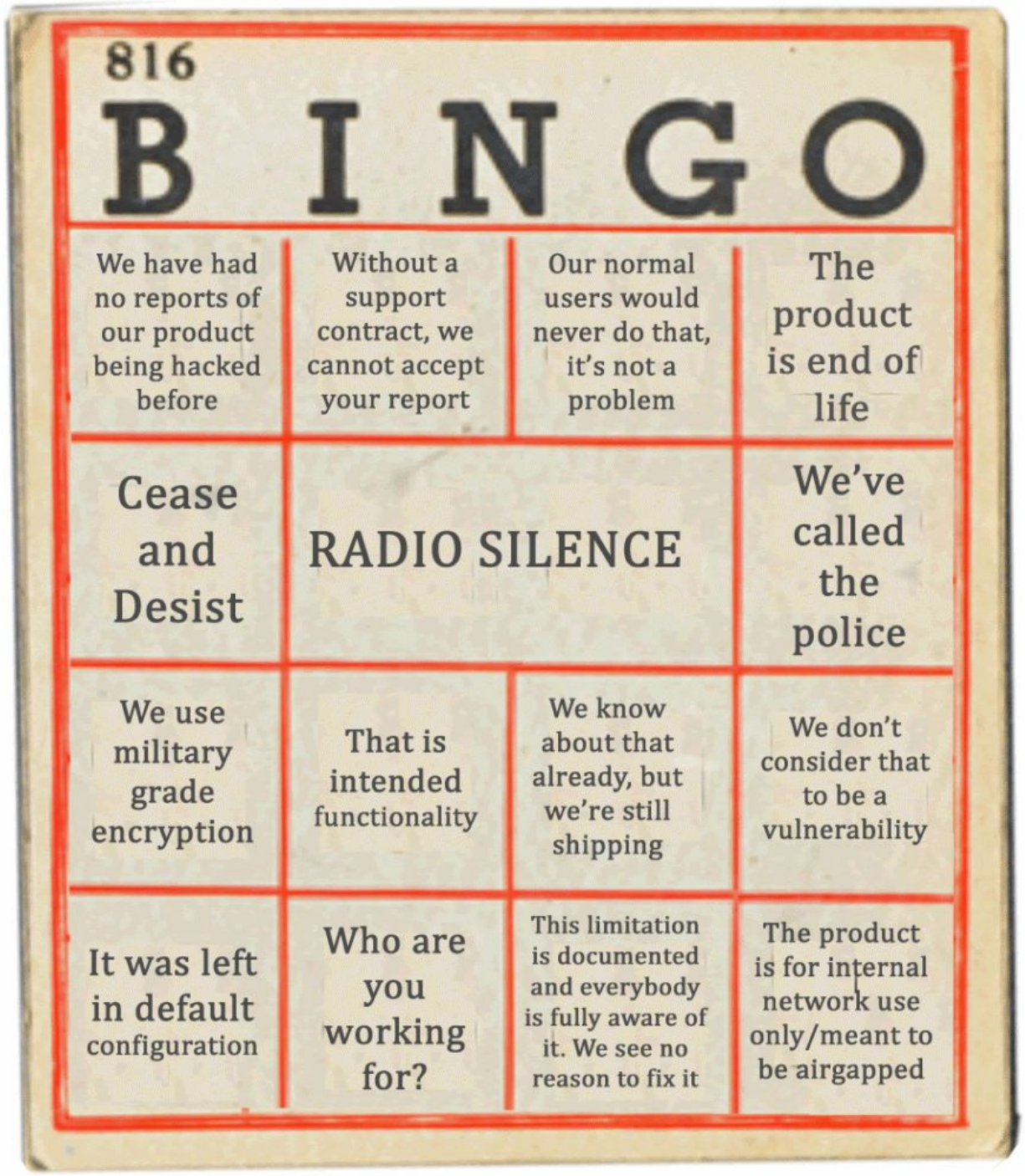
Wider experience

Authentication bypass vulnerability discovered on a publicly-facing website:

- Researcher tried contacting the company through various means
- No response, unsure if it was ignored or just didn’t reach the right person
- No official VDP making submission challenging
- Researcher resorted to Social Media provoking a reaction
- Story gets a bit weird at this point:
  - An official submission was made
  - Things were fixed
  - Accusations on both sides
- My understanding is that the bridges between them are still broken.

Buzzword Bingo!

Courtesy of Ken Munro - PTP



Receiving a submission….

Do:

- Have a Vulnerability Disclosure Program (remember, it's more than a web page)
- www.<yourdomain>.com/.well-known/security.txt
- Consider making security@<yourdomain>.com active and is monitored
- Do engage with researcher submissions
- Communicate! Communicate! Communicate!
- Use legal representation where necessary
- Agree on disclosure – timelines, message, details, etc.
- Follow the agreed plan

Don't:

- Ignore the problem
- Belittle the concerns in the submission
- Force the NDA
- Make threats or intimidation
- Go after the researcher's reputation
- Don't rely on security by obscurity – it doesn't work!

When you submit a vulnerability….

Do:

- Check if they have a Vulnerability Disclosure Program. Follow it!
- Engage responsibly and make every effort to go through formal channels
- Consider using Aviation-ISAC
- Communicate full details and reply to all questions
- Leave emotion at the door, stick to facts
- Understand the 60 day ‘rule’ may not apply. Fixes can take years!
- Understand you may have to enter a restrictive agreement to know more information

Don’t:

- Get upset when full mitigation details cannot be shared with you
- Breach your NDA!
- Ignore laws
- Disregard agreements or requests
- Use it as a business opportunity!

Thank you!

Questions?

