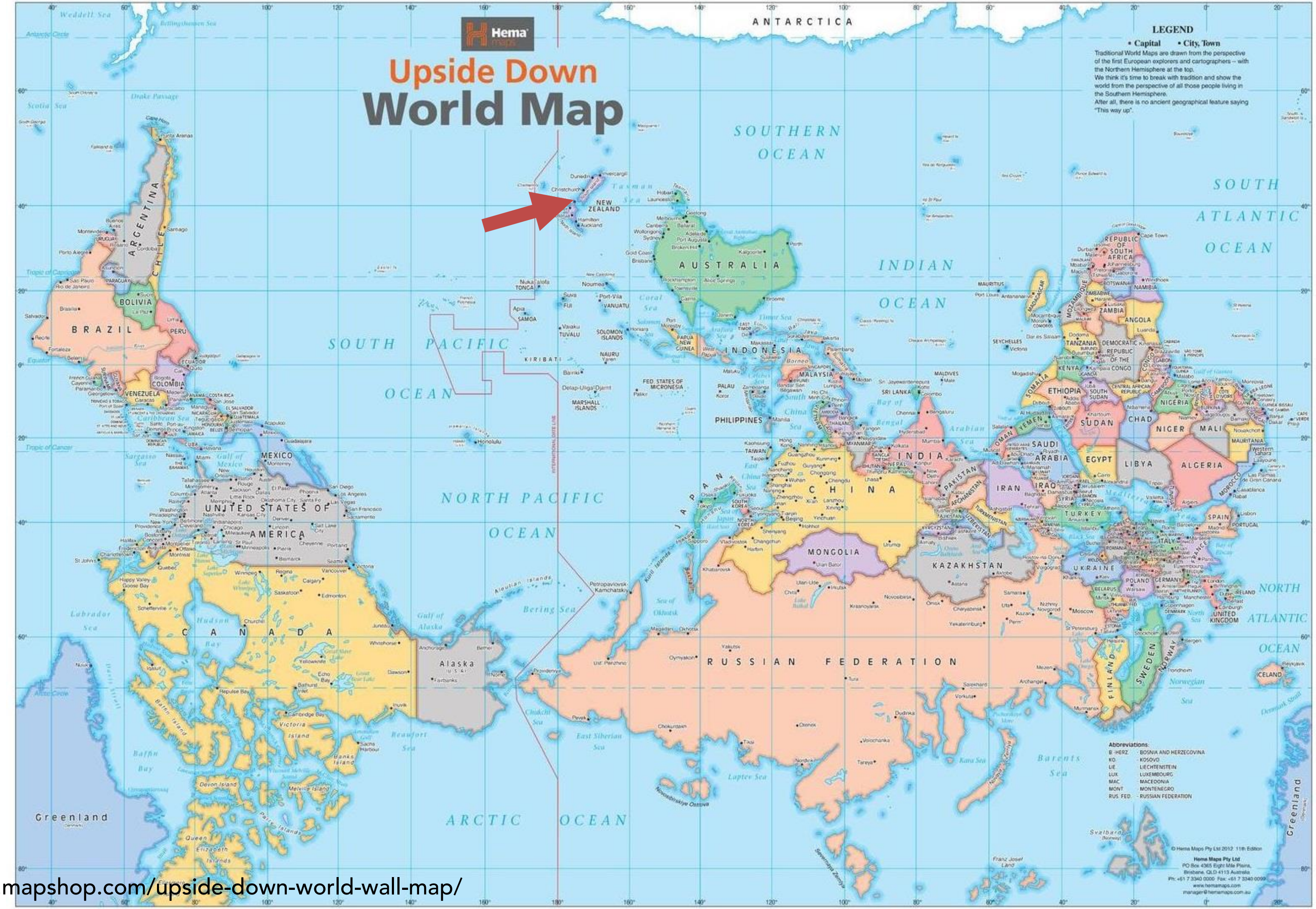
A look at GA EFBs

David Robinson/Karit
@nzkarit

Aerospace Village August 2020

whoami

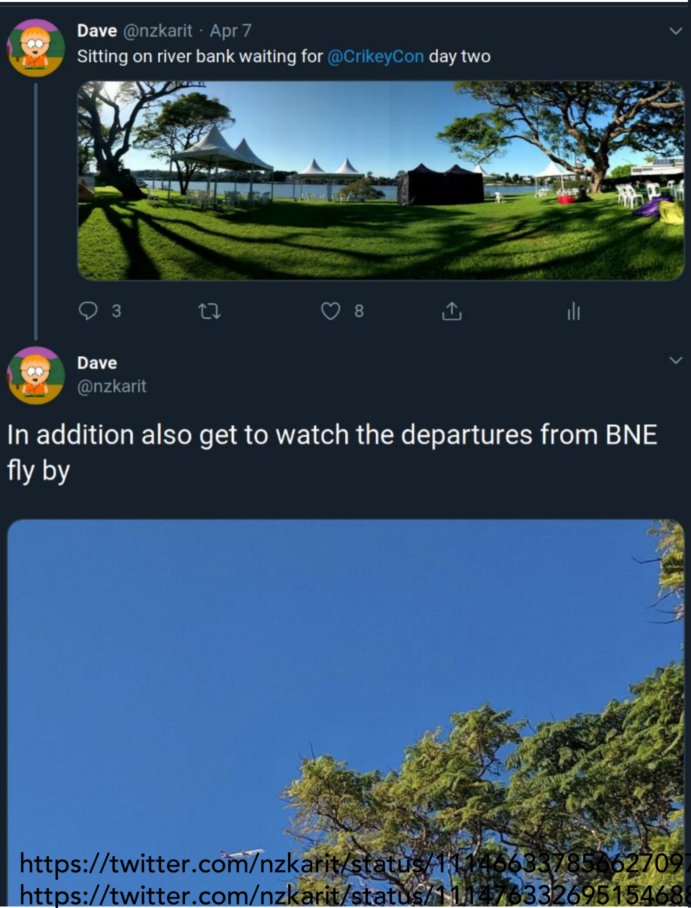
- David Robinson
- Karit
- @nzkarit
- Pen Tester



Traditional World Maps are drawn from the perspective of the first European explorers and cartographers – with the Northern Hemisphere at the top.
We think it's time to break with tradition and show the world from the perspective of all those people living in the Southern Hemisphere.
After all, there is no ancient geographical feature saying "This way up".

https://www.mapshop.com/upside-down-world-wall-map/

Might enjoy hacking and aviatic

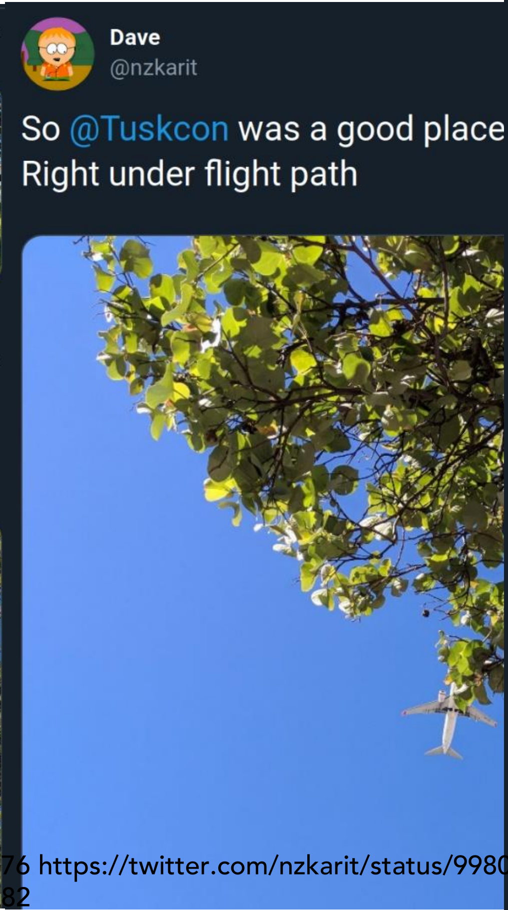


Dave @nzkarit · Apr 7

Sitting on river bank waiting for @CrikeyCon day two

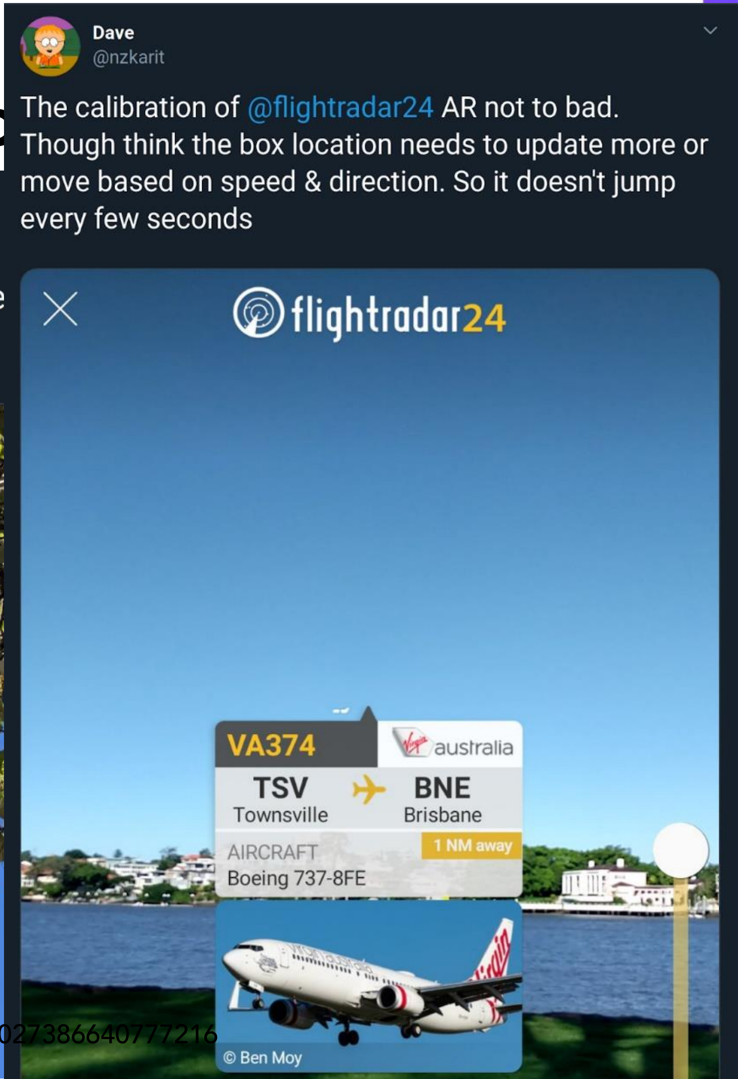
Dave
@nzkarit

In addition also get to watch the departures from BNE fly by



Dave
@nzkarit

So @Tuskcon was a good place
Right under flight path



Dave
@nzkarit

The calibration of @flightradar24 AR not to bad. Though think the box location needs to update more or move based on speed & direction. So it doesn't jump every few seconds

flightradar24

VA374 australia

TSV Townsville → BNE Brisbane

AIRCRAFT Boeing 737-8FE

1 NM away

© Ben Moy

https://twitter.com/nzkarit/status/1114663378566270976 https://twitter.com/nzkarit/status/998027386640777216
https://twitter.com/nzkarit/status/1114763326951546882

Today

- Electronic Flight Bag (EFB) in the General Aviation (GA) Cockp
- Example issues
- How to mitigate these issues

https://www.aopa.org/news-and-media/all-news/2020/march/flight-training-magazine/ol-power-up

Scope

- Going to look at a high level of the types of vulnerabilities
    - Opposed to looking at individual vulnerabilities
- Additionally not going to be naming vendors, etc

Frame of Reference

- When discussing issues in this I am thinking about:
- CIA Triad:
  - Focus on Integrity and Availability
- Even if tin says “Don’t use for navigation, safety, etc purposes” people are going to
  - So need to make it safe

Goal

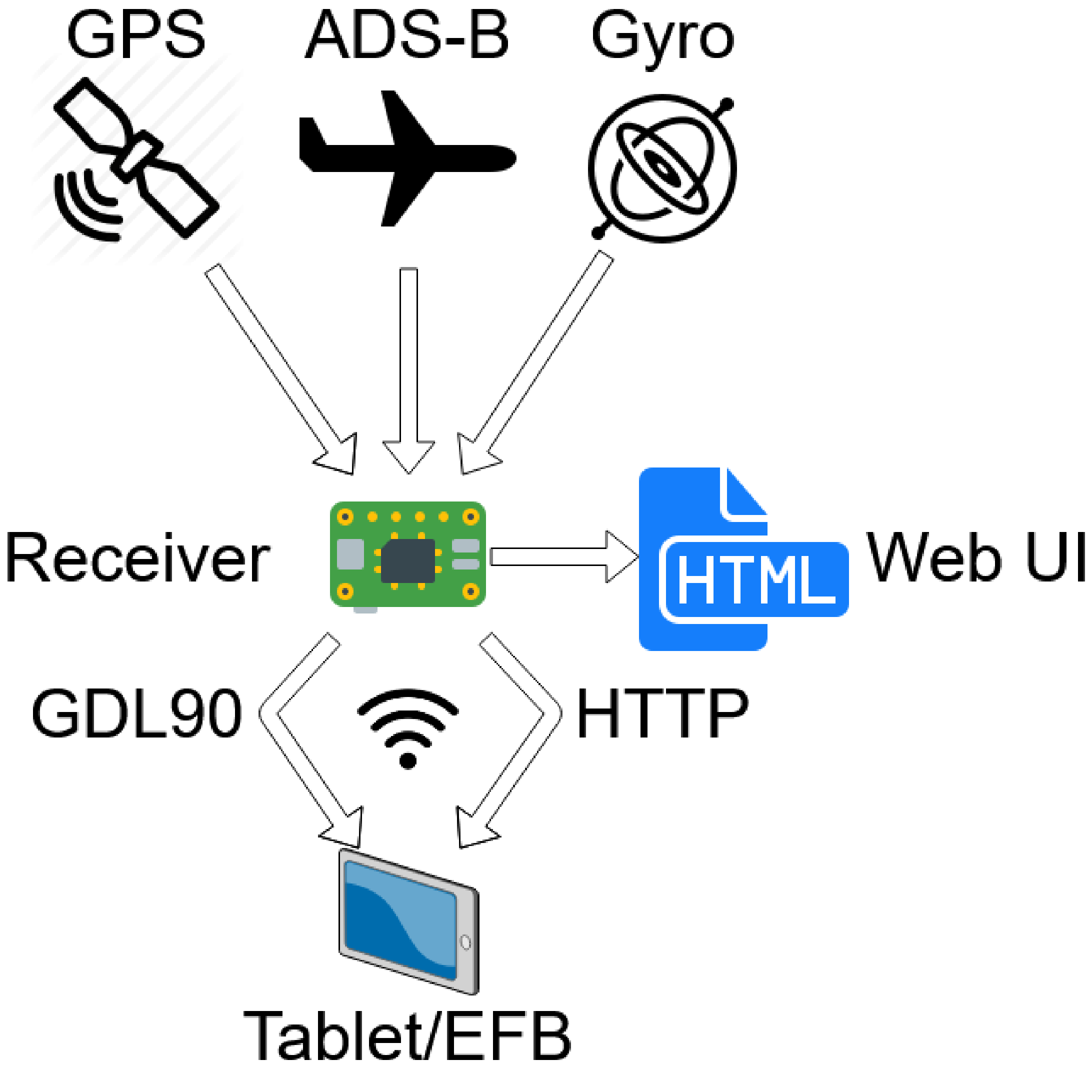
- To help people produce for robust and secure systems for their customers
- With a focus on people working with GA EFBs

Background

- To an IT security professional most of these will not be new issues
- These are though, common issues when a new industry makes their devices more connected
  - This is not first industry we have seen these issues in and nor will it be the last

What is an EFB (GA)

- Often on a tablet
- Combination of:
  - Flight Charts
  - Airport Charts
  - Attitude and Heading Reference System (AHRS)
  - Situational Awareness
    - ADS-B In, FLARM



GPS

ADS-B

Gyro

Receiver

Web UI

GDL90

HTTP

Tablet/EFB

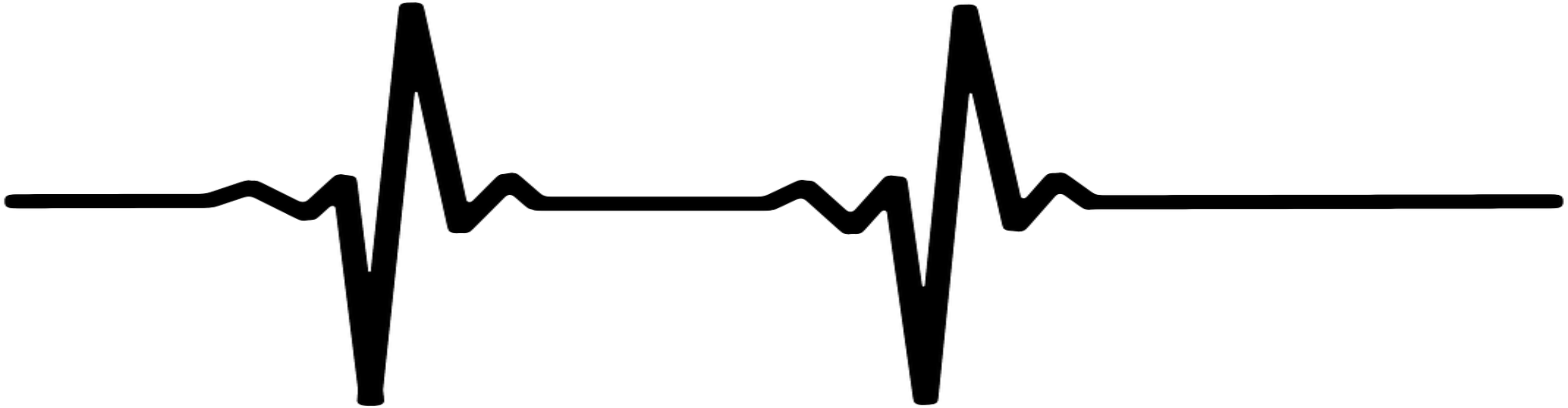
My Testing Setup

- I tested only on my own devices/hardware
- Where radio was involved I:
  - Used a faraday cage
  - Turned Tx power down
  - Used non Aviation Frequencies
  - Directly connected transmitter to receiver with cable
- No internet connection while performing tests

Example Issues

- Heartbeat Messages
- Validity of Data
- DoS Scenario – Situational Awareness
- GPS Spoofing
- Integrity of Data
- Insufficient Device Hardening
- Password Management

Heartbeat Messages

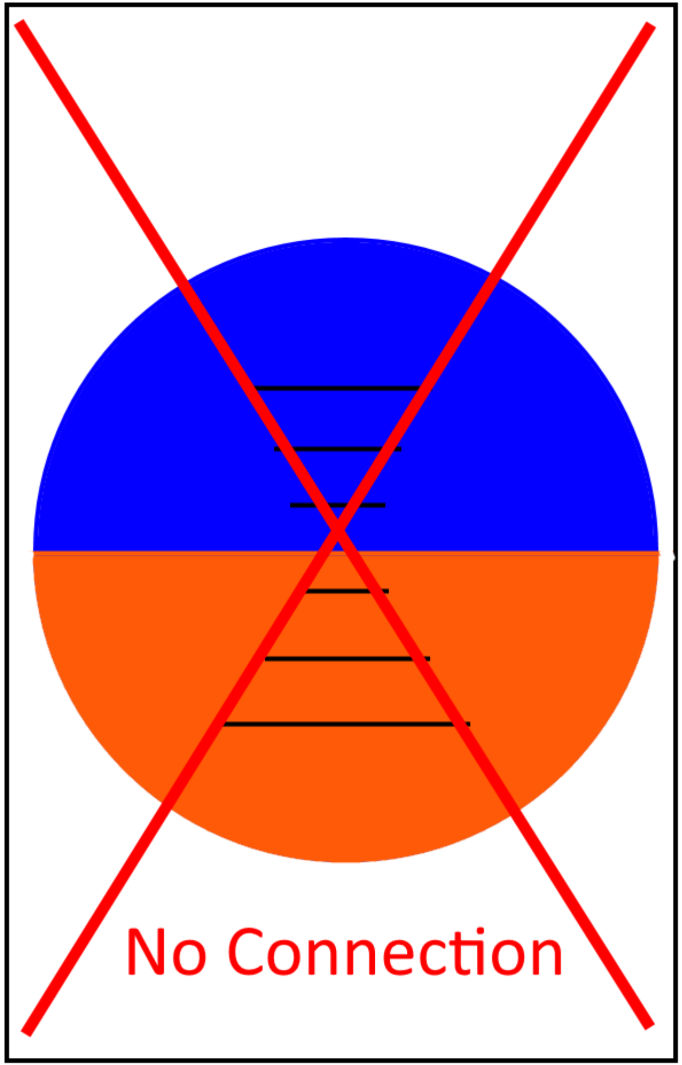


https://www.needpix.com/photo/download/248067/heart-rate-pulse-live-line-wave-frequency-medical-rhythm-free-pictures

Heartbeat Messages

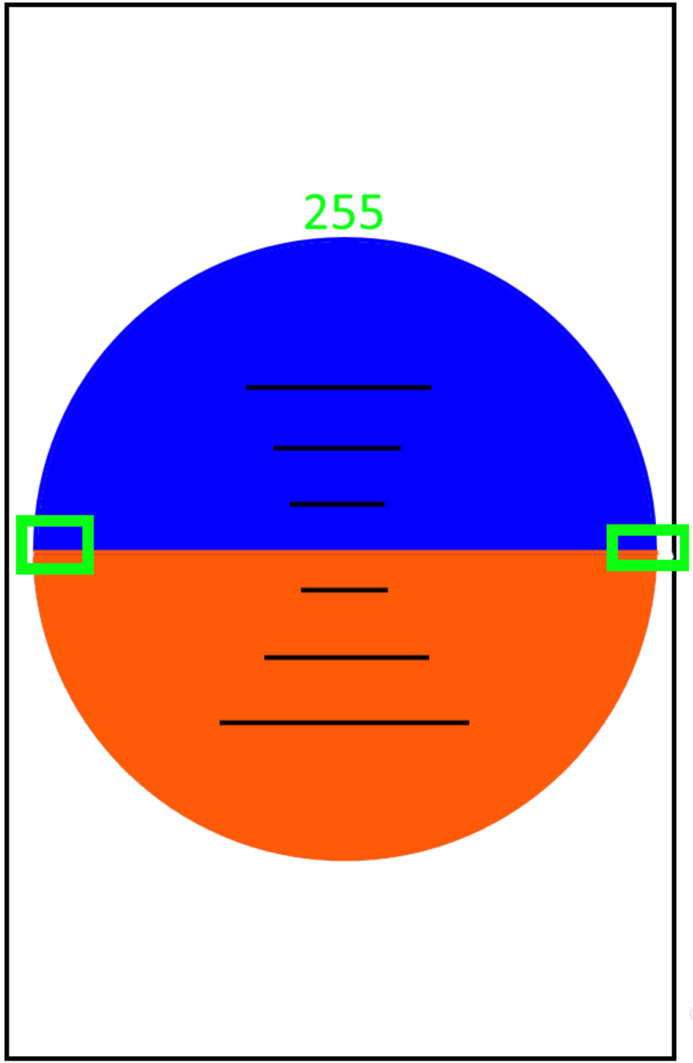
- The receiver will often send Heartbeat messages
- The EFB should use this message to inform the pilot when there is an issue

Start EFB, Receiver Off

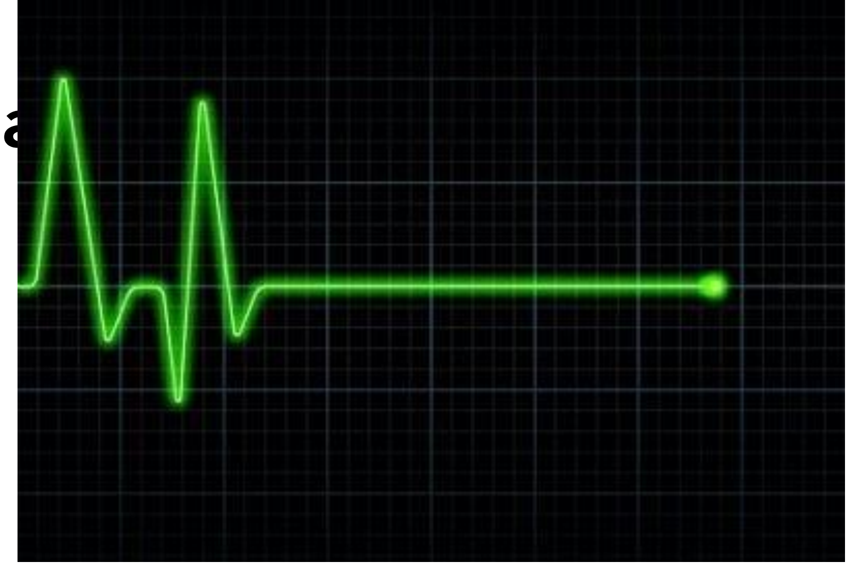


Start Receiver

- Red X goes away
- Displays the data



Stopping the Heartbea



- Turn off receiver
- Tamper with data

- What would you expect to happen?
  - Inform the pilot? E.g. bring back red cross
  - Just continue, like nothing has happen?

https://theevolutionofeducation.blogspot.com/2012/04/leadership-flatline.html

Who picked "Just Continue"?

- Well that is what happened.
- If a system is in a degraded state the pilot should be informed

Solution – Heartbeat Messages

- Monitor the data being received by the EFB
    - This is an ongoing check not just a start up check
- Inform the pilot when:
    - It stops being received
    - If data which was present in earlier message is no longer there

Validity of data

https://commons.wikimedia.org/wiki/File:Green_tick.svg

Validity of Data

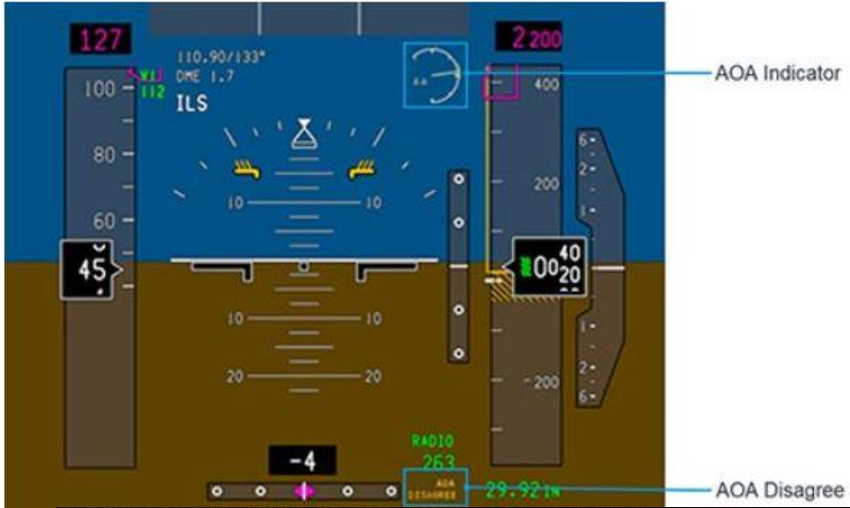
- The data the EFBs receive from the receivers may not always be valid
- Receivers have faults, so send bad data
- Corruption may happen in transit
- Malicious individual could inject malicious data

Example

- Heading
  - Normally 0 to 359
- What happens with heading >360?
- Sent an EFB a heading of 450 degrees
  - Was remapped to 90 degrees

Outside Example

- 737 Max AoA disagree was an optional extra
  - Displays warning when the 2 sensors are different
  - Lets the pilots know when they can't rely on it



http://www.b737.org.uk/mcas.htm https://boeing.mediaroom.com/image-gallery?cat=32#gallery_gallery_0:20348

EFB Behaviour

- EFB don’t appear to have a indication when input data is not valid
  - We be good to see this type of warning when data in Receiver or EFB starts to disagree or go out of bounds

Solution – Validity of Data

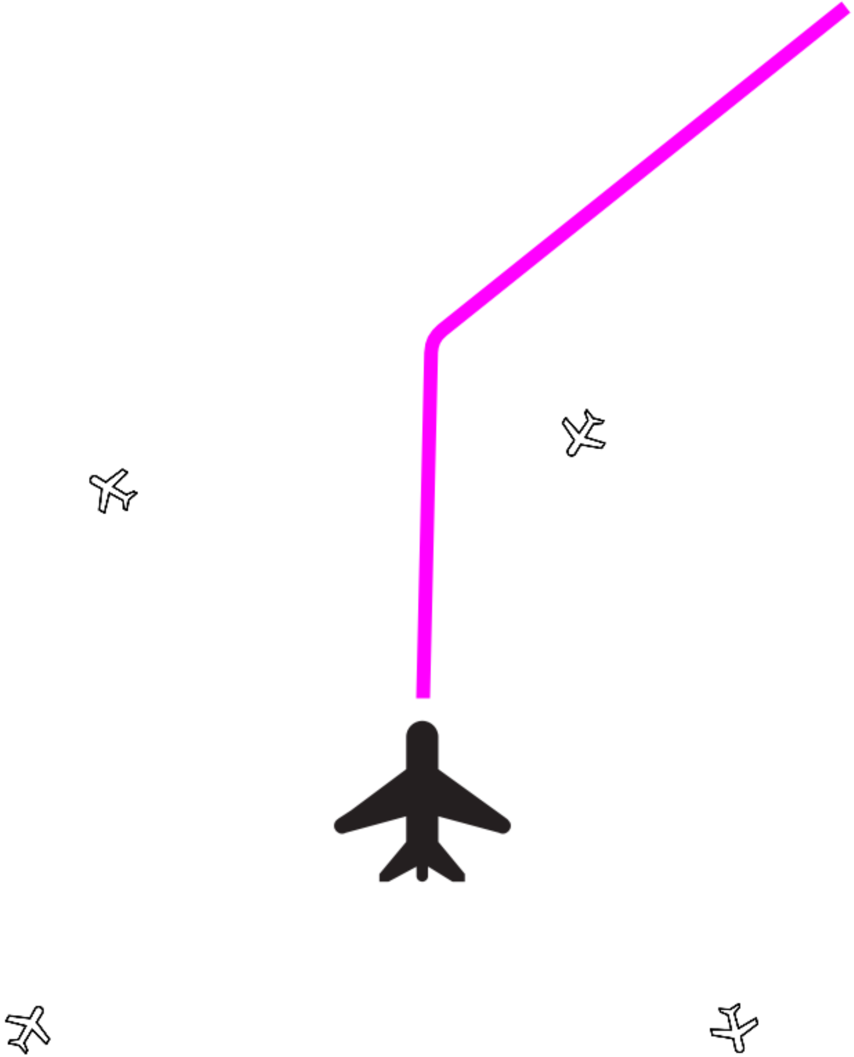
- Know that expected should look like
  - Have the expected range of data and check when out of range
  - Look at trends in the data, is it changing too fast?

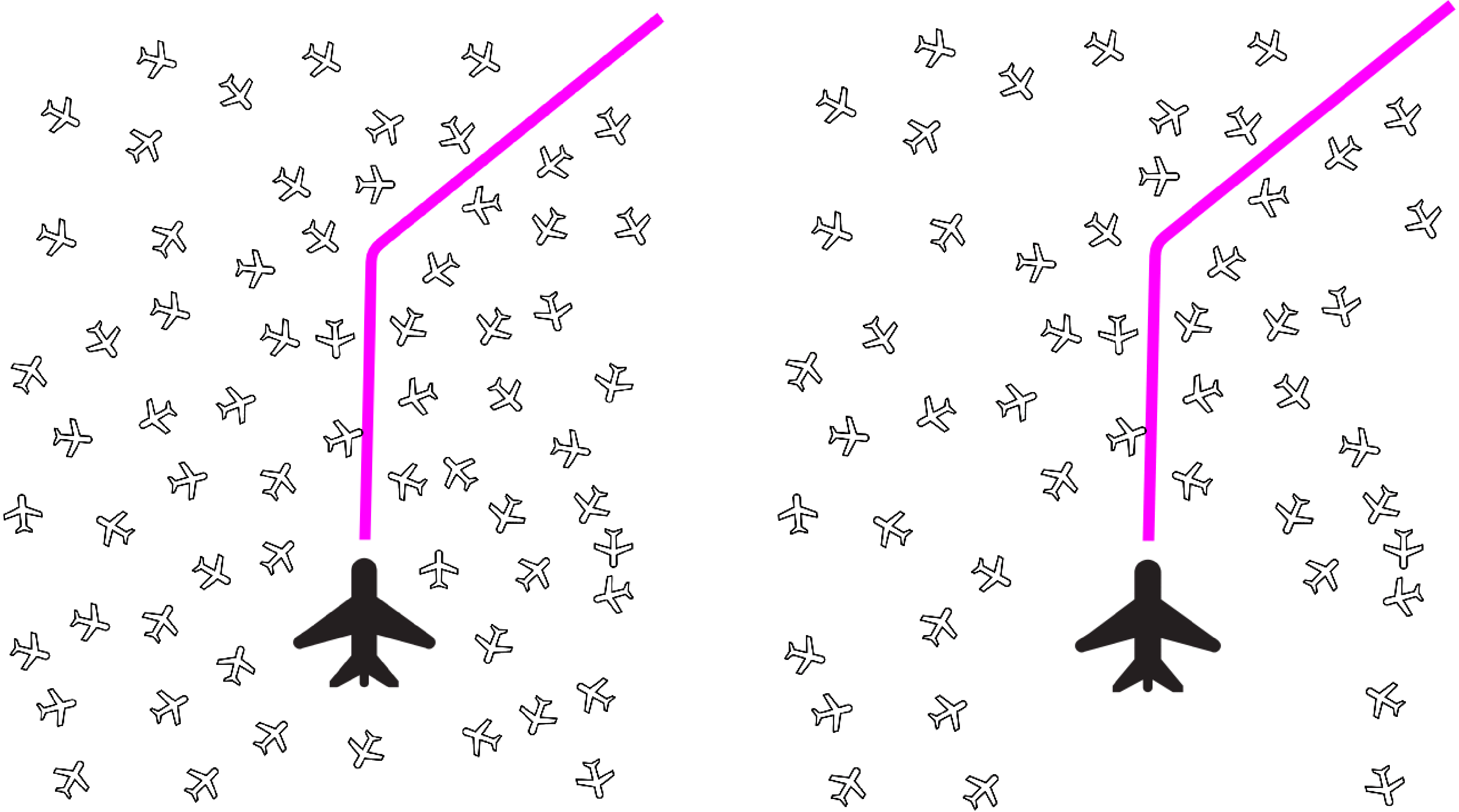
DoS Scenario – Situational Awareness

Situational Awareness

- Some EFBs display a moving map with ADS-B targets to help with situational awareness.
- With SDR can transmit ADS-B Out
- Renderman has discussed this previously

Situation Awarenes



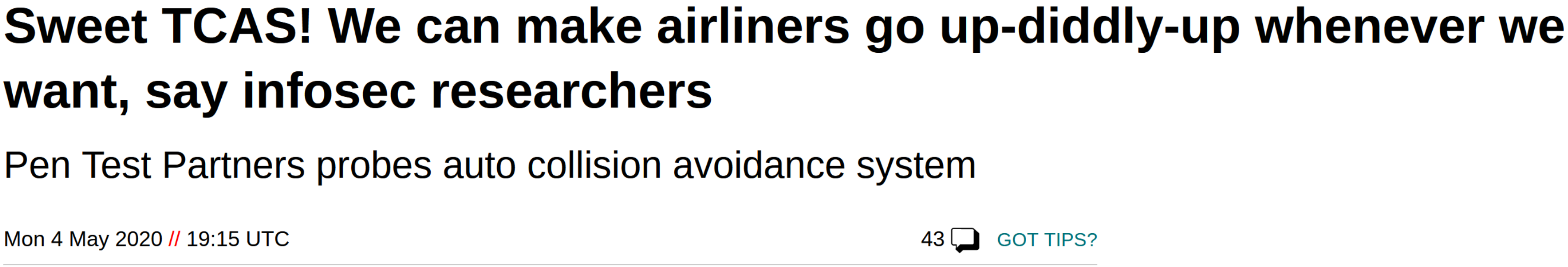


Planes missing

- Was not always the furthest ones which disappeared
- I could not determine a pattern other than timing
- Same input resulted in different outputs

Combine with TCAS

- Could combine the malicious ADS-B Out with TCAS
- Can make the two sources correlate with each other



Sweet TCAS! We can make airliners go up-diddly-up whenever we want, say infosec researchers

Pen Test Partners probes auto collision avoidance system

Mon 4 May 2020 // 19:15 UTC

https://www.theregister.com/2020/05/04/tcas_spoofing_pen_test_partners/

Solution - DoS Scenario – Situational Awareness

- If ADS-B In receiver not broadcasting all planes needs to flag the degraded state
- If EFB should alert the pilot if it is receiving too many different planes and is not displaying all the of them

- Make the ADS-B In antenna have direction capability like some TCAS systems
  - to cross reference actual direction with

GPS Spoofin

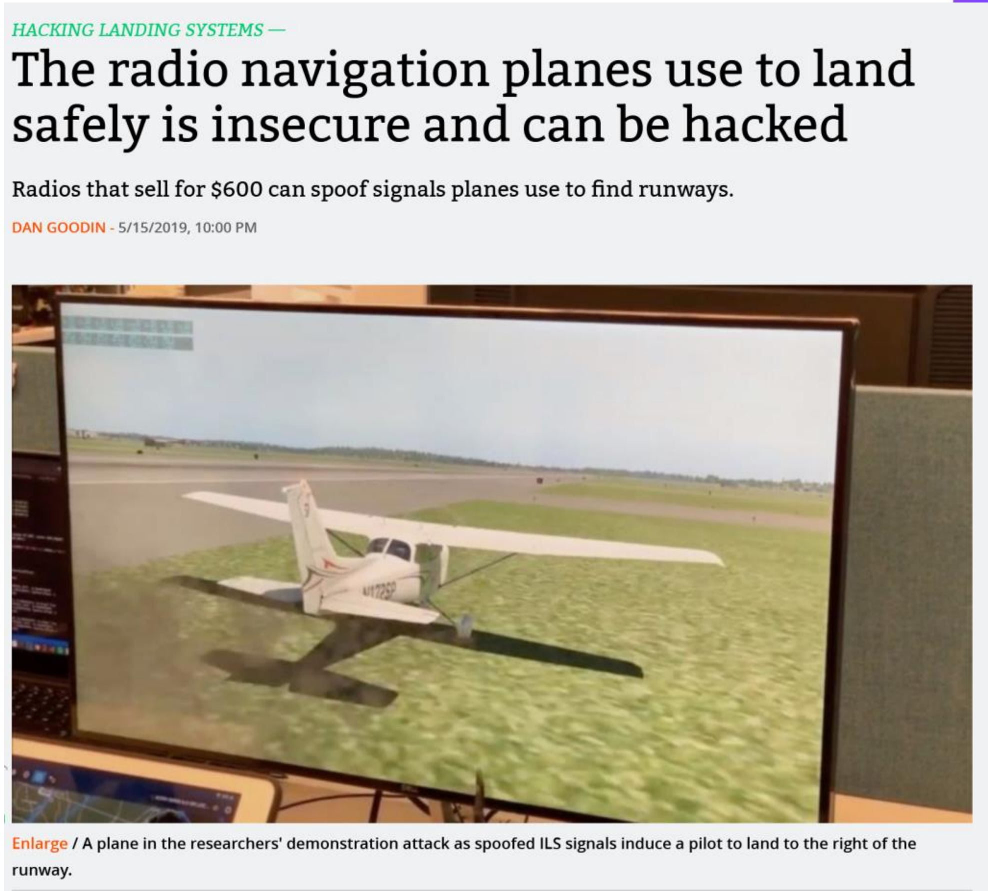
https://www.schriever.af.mil/News/Article-Display/Article/734934/a-short-history-of-gps-development/

GPS Spoofing

- From my testing the case of Jamming and signal loss is handled
  - EFB normally had indicator that had GPS fix
  - And indicator when no GPS fix
- Case of malicious signals not the case

ILS

- When combine with the ILS spoofing discussed at last year’s Aviation Village
  - GPS/GNSS RNAV was the cross check



HACKING LANDING SYSTEMS —

The radio navigation planes use to land safely is insecure and can be hacked

Radios that sell for $600 can spoof signals planes use to find runways.

DAN GOODIN - 5/15/2019, 10:00 PM

Enlarge / A plane in the researchers' demonstration attack as spoofed ILS signals induce a pilot to land to the right of the runway.

https://arstechnica.com/information-technology/2019/05/the-radio-navigation-planes-use-to-land-safely-is-insecure-and-can-be-hacked/

Detecting GPS Spoofing

- In a talk from 2017 I did a range of GPS spoofing research
- One thing which came of that was GPS Snitch
  - https://github.com/zxsecurity/gpsnitch
  - It is possible to detect GPS Spoofing

Aspects to consider

- If time suddenly changes
- If location jumps more current speed allows
- Signal Strength
  - Overall Strength
  - Range of Strengths
- Signal Direction

Solution – GPS Spoofing

- Monitor GPS for abnormalities
- Show a indicator like the one when have no GPS fix

Integrity of Data

Integrity of Data

- Nearly all the data is clear text
- There is an encrypted version of GDL90 but did not actually find anything using it
- By default the Wi-Fi often clear text

Integrity of Data

- No shared key material on first pair of EFB and Receiver
  - So can switch out the receiver and no error
- In formation flying may connect with friend’s plane
  - If using the same system with same SSID

Solution – Integrity of Data

- Use the encrypted version of GDL90
- When first pair a EFB and a receiver exchange key material
  - Sign every message
  - If message not signed disregard
  - Ensure protect against replay attack

Insufficient Device Hardening

Networking configuration

- Receivers had internal services bound to 0.0.0.0
  - Things like fan controller
- Weak Wi-Fi configs
  - No PSK
  - No PMF/802.11w
    - Stops deauth attacks

Service configuration

- Weak SSHd configs
  - Why port forward allowed
  - Root login
  - Etc
  - In most cases doesn’t even need to be on by default
- Web Config UI no password on first use
  - Security in depth with PSK on Wi-Fi

Solution - Insufficient Device Hardening

- Seek advice on hardening configurations
- Follow hardening guide for components which are using

Password Management

https://commons.wikimedia.org/wiki/File:Hacking_password_illustration.jpg

Password management

- Hardware not prompting for password change on first use
- Hardcoded Wi-Fi PSK
  - PSK off by default but enable message said remember it only will see this once.
  - But always gave the same PSK

Companion Websites

- I did not test these
- I registered for an account
  - Sometime this was required to get the EFB to work

- Some EFB had signups as allowed to submit flight plans, subscriptions, etc

Websites

- Got emailed password in cleartext
  - Often means not stored correctly in DB
- Allows weak passwords
  - Even said can’t used special characters
  - My first thought when see that is not hashing and SQL Injection (didn’t test but experience)

Solution – Password Management

- OWASP Foundation provides some great guides on password storage and authentication
  - https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html
  - https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
  - https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html

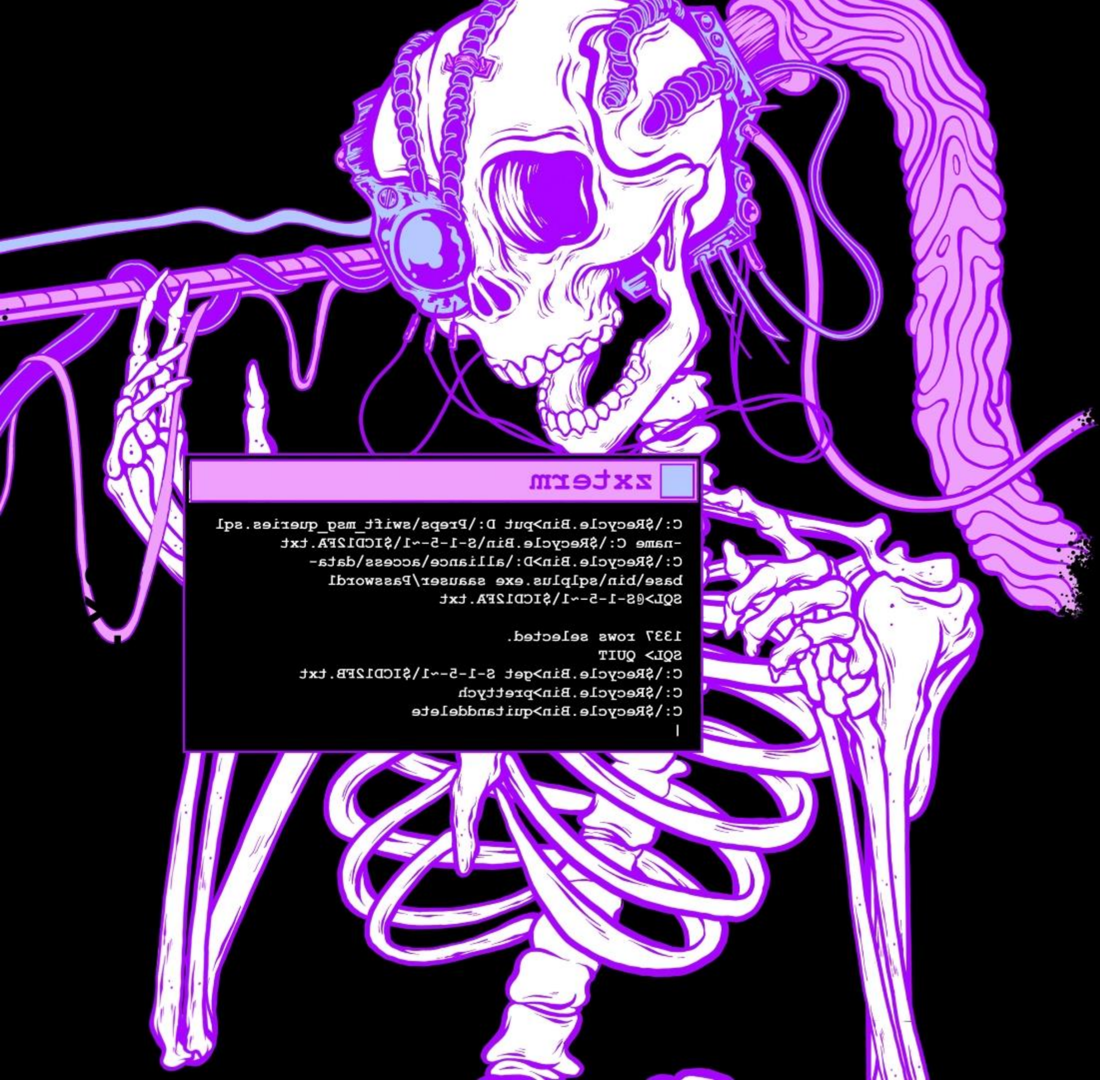
Summary

- Hopefully the example issues and solutions are of help
- In addition hopefully in future development there is more thought put into “What could a malicious individual do? Does this affect the integrity or availability of the system?”

Help from the security industry?

- What help is needed from the security industry?

- Example Test Cases for all these which EFB and receiver manufactures can use
- Developing Test Harnesses which have the malicious content in them so testing is easier



```
C:/$Recycle.Bin>put D:/Preps/swift_msg_queries.sql
-name C:/$Recycle.Bin/S-1-5-~1/$ICD12FA.txt
C:/$Recycle.Bin>D:/alliance/access/data-
base/bin/sqlplus.exe saauser/Password1
SQL>@S-1-5-~1/$ICD12FA.txt

1337 rows selected.
SQL> QUIT
C:/$Recycle.Bin>get S-1-5-~1/$ICD12FB.txt
C:/$Recycle.Bin>prettych
C:/$Recycle.Bin>quitanddelete
|
```

Thanks

David Robinson
ZX Security

@nzkarit