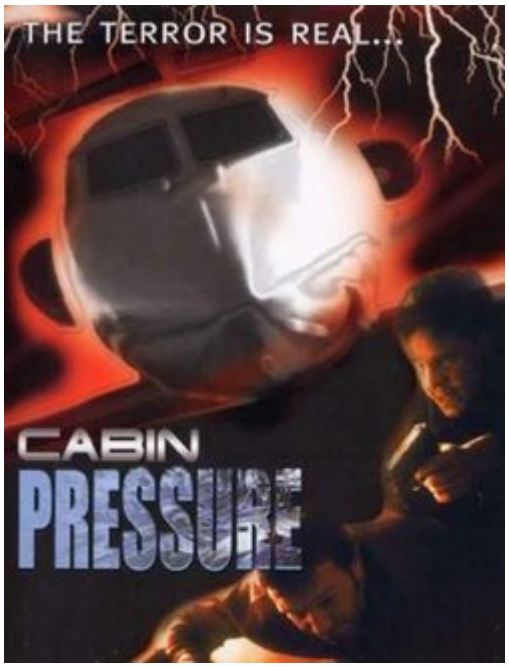
Squawk 7800 for Hacked

OPSGROUP Team
13 April, 2021



An airplane is circling over Seattle. Onboard, the Captain, Reece Roberts, is desperately trying to control it, but cannot – she is locked out from the flight control systems because the main computer has been hacked. It is a race against time for the crew to regain control before they run out of fuel. Dom Dom DOOOOMMMMM!!



Not real, just a movie, but…

This might sound like the plot from a terrible movie (it is), but how possible is this, and are there any mechanisms in place to prevent it?

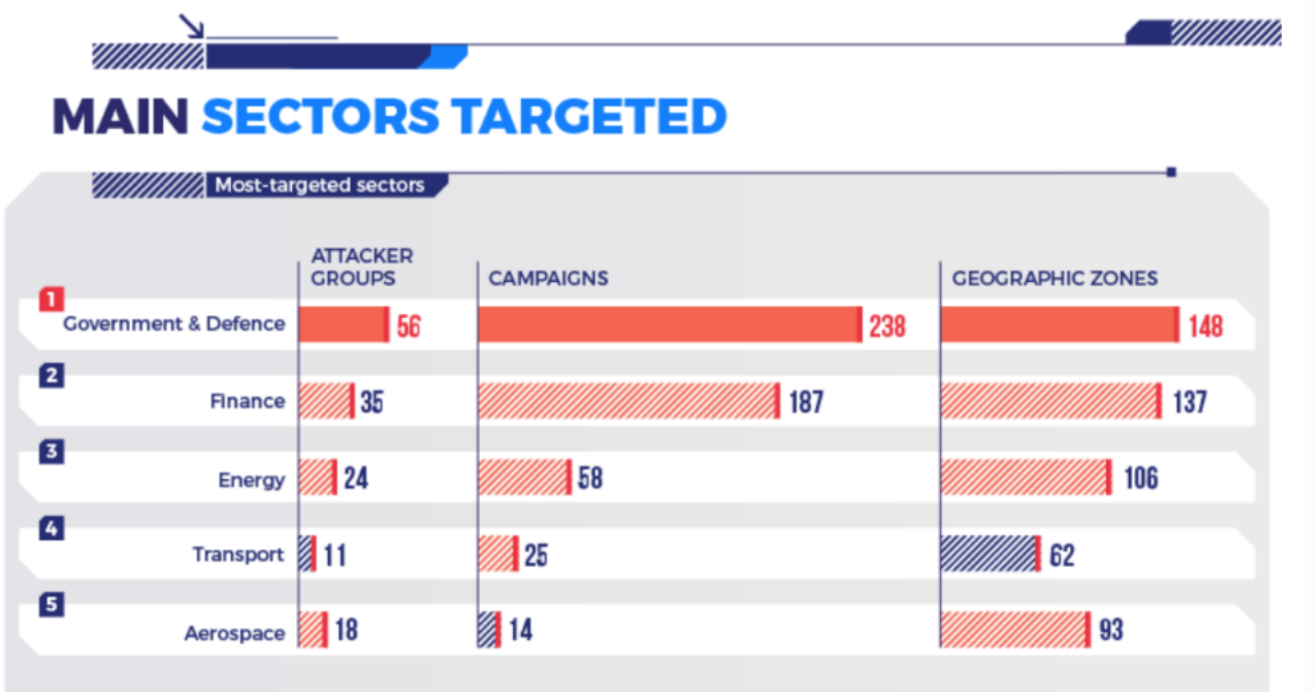
Hack attack

Back in 2015, a cyber security expert, Chris Roberts, was detained by the FBI after making some claims on social media about hacking into an aircraft computer and briefly assuming control of it. According to Roberts he had hacked into several planes over a four year period, using the in-flight entertainment system as his way in.

On this particular occasion, Roberts claims he managed to **overwrite some code and issued a "climb" command** to the airplane which then caused one of the engines to increase thrust. His actual statement was that he made the airplane "fly sideways" (which possibly discredits the whole story just a little).

This is not the only claim of aircraft hacking though. In 2016, a **Boeing 757's system were also breached**, and this one was slightly more disturbing because it actually, definitely happened. It was also less worrying because the aircraft was on the ground and the whole thing was carried out by the US Department of Homeland Security as an exercise to see how possible a hack attack actually would be.

The Aerospace sector **is the fifth most targeted sector for cyber-attacks**. A high level then, but while some of those attempts are aimed at aircraft flight control computers, and an equally small number at infiltrating airport infrastructure systems, **the large majority are of the data gathering nature** – attempts to steal sensitive passenger info, credit card data and that sort of thing.



Taken from a Thales report.

How serious are we talking?

Our aircraft are intelligent. The computer brains that run them are complex beasts made up of multiple data generating sensors, and just as many parts giving out orders to various aircraft systems. Take the FADEC on an engine – this is a self-monitoring, automated system. It controls the engine start, deciding when to open valves up, when to add fuel. It also monitors parameters and can stop a start, run a cooling cycle, and try all this again without pilot intervention. The system also controls inflight restarts.

Rolls-Royce launched an 'intelligent engine' concept in 2018 – an engine so connected that it has the basic AI algorithm "intelligence" to assess, analyse and learn from its experiences, as well as those of its "peers"

(other engines that all share their data).

All this level of automation is great, but **what if it is no longer in control**, and is being controlled with the pilot effectively locked out?

Then there is the connectivity

Aircraft are increasingly digitalized and increasingly connected, and these connections might be less secure than we think. One highlighted "weakness" in aircraft onboard systems is the encryption levels within the comms and reporting systems. You might point out that aircraft are fairly visible on Flightradar, but this only gives general whereabouts, and transponder data is no longer shared. Being able to **pinpoint exact locations in real time** has far greater consequences if the wrong people are able to access this information.

There is growing speculation that Malaysia Airlines Flight 370 may have been electronically hijacked, or at the very least had its position spoofed leading to the initial confusion over its whereabouts, and later the difficulty finding the crash site.



Aircraft are increasingly connected to the 'open world'

The good news

The good news is there are protections within aircraft systems. First up, there is **no way to access a critical system via a non-critical one.** Network architecture prevents this and various experts have stated it is impossible to move from, for example, the in-flight communications system to the avionics.

Airbus incorporate a switch in the flight deck – the NSS (Network Server System) gatelink pushbutton is effectively an added **'disconnect' which separates all cockpit systems from the 'open' world**, cutting off any potential link to the aircraft flight management systems should a threat be perceived.

Then there is the risk of **“locking” the pilot out** – gaining access of a system and sending commands to it is one thing, but pilots have the ability with most systems to disconnect and get back to basics. For a hacker to lock a pilot out – prevent them from disconnecting – this would require a command that is not currently in the system and this level of hacking and re-programming is not, most suggest, all that feasible.



The avionics bay

The bad news

There are other ways to disrupt operations.

GPS jamming is not direct interference, but the impact it has on aircraft systems is a known one – with a jammed GPS, **aircraft lose the ability to navigate with accuracy** and must rely on dated radio navigation systems. Not such a big issue, but removing the capability for an aircraft to carry out an RNP or RNAV approach means they are reliant on older ILS equipment, or having to fly non-precision approaches.

ILS equipment relies on both ground and aircraft systems, meaning there are much more “parts” which can fail. These systems are also older and require more maintenance on the ground meaning the likelihood of one part malfunctioning is higher, and when it does, the **level of safety redundancy for aircraft which have had GPS jamming problems is suddenly really reduced.**

The risk of interference to GPS and radio signals also creates a vulnerability in UAV operations. The controllability of an aircraft might not be in question, but the ability of a hacker to take over and control a UAV – and potentially “control” it into an aircraft – is a growing threat.

A report looking into potential airport weakness identified a large number of “weak spots” where targeted hack attacks might result in disruption. The airside points ranged from spoofed ILS signals to changing airplane signatures on docking system from larger to smaller aircraft, reducing the wingtip clearance margins and safety significantly.

What is being done?

Technologies to prevent UAVs in airports is well underway with systems in place already at many major airports, and the FAA trialling more this year. Solutions to GPS jamming are also a high priority with several conferences and work groups already taking place, identifying both the threat and the root cause of why jamming takes place.

As for the direct cyber security risk to aircraft, this is not a new “idea”. The FAA moved it in the right direction with their **Aircraft Systems Information Security Protection (ASISP) initiative** in 2015. This initiative asked the questions, and asked manufactures to start thinking up answers, and they are responding. Manufacturers of major avionics, entertainment systems, communication systems, and aircraft are all analyzing the risks, and upping the protections, securities and preventions.

We might not see them in our aircraft, but they are there, and until aircraft become completely secure we still have that last trick up our sleeve – the one where we just **turn it off** and get back to basics and fly it ourselves.

So ‘Cabin Pressure’ might just be collection of movie cliches surrounding a troubled plane that no-one takes seriously, but the threat of cyber terrorism in aviation is one that everyone else is taking very seriously indeed, and for good reason.