Is cyberjacking a new threat to air travel?

July 13 2015

When Malaysia Airlines flight MH370 vanished en route to Beijing in March 2014, the horror and mystery of the story captivated the public. And as with any mystery, the lack of a definitive answer left a void for speculation and conspiracy theories. Was the aircraft shot down? Was it hijacked and flown to an unknown location? Was the plane's computer system somehow hacked allowing it to be controlled remotely?

It was this latter theory that most interested Professor David Stupples of City's Department of Electrical and Electronic Engineering. Professor Stupples is an expert in networked electronic systems and, prior to becoming an academic, spent many years developing military surveillance systems for the Royal Signals and Radar Establishment. He also designed secure communications for surveillance satellites and air defence systems for the Hughes Aircraft Corporation.

The MH370 mystery got him thinking: was it possible to 'cyberjack' a civilian aircraft? If so, are we at the beginning of a new and terrifying era for commercial air travel?

To answer these questions, it's useful to look at how aircraft have evolved. In the 1970s the US government developed the F-117 fighter plane, the first designed around stealth technology and therefore undetectable by radar. Unfortunately the design made the aircraft aerodynamically unstable: the only way it could be flown was if it had a computer on board.

The computer flies the plane

By the 1990s, Airbus had introduced computers on commercial aircraft and today, with the introduction of the firm's 318, 319 and 320 series, its planes are now almost totally computer controlled. As Professor Stupples says: "The pilot flies the computer and the computer flies the plane."

Today's modern aircraft have numerous systems, including those for flight controls, automatic pilot, navigation, communication, engine management and even passenger entertainment. If these systems can be accessed by anyone with malevolent intentions, the consequences could be disastrous.

In recent years there have been numerous cyberjacking scare stories. In 2008, for example, the United States Federal Aviation Authority reported that the computer network in Boeing's 787 Dreamliner passenger compartment was connected to the aircraft's control, navigation and communication systems. This grave security concern was subsequently resolved by Boeing.

And in April this year, a security researcher was prevented from boarding a United Airlines flight after tweeting that he could hack the

plane's systems. So is it possible to cyberjack a modern civilian aircraft? Professor Stupples says yes – but there's a very large 'but'.

A tough nut to crack

"Cyberjacking by a passenger is going to be exceedingly difficult," he says. "He can't come through the Wi-Fi system, that's not possible. He could perhaps interfere with the navigation but the aircraft would warn you. All the systems are totally integrated. How then could he take control of an aircraft? The only way is to get malware on board."

Malware is software designed to cause harm to a computer system, for example to disrupt it or steal sensitive information. Most of us have received suspicious-looking emails asking us to open attached files: these are often malware viruses ready to infect our PCs.

"One way to get malware on board would be for the software developers to put it on when they develop the software," he adds. But of course that means having a rogue employee working for the software company. "For someone to develop the malware who is outside the aviation industry, that is again a difficult task because the systems are all totally integrated. The other way is to load the malware by accessing the aircraft's on-board electronics bay. This is possible but access controls are very sophisticated."

Professor Stupples and his colleagues recently carried out research into the most likely ways that a system can become infected with malware. They calculated that the biggest threat came from a rogue or coerced employee, backed by serious organised crime or even a state.

So what can companies do to protect themselves? Can a system ever be totally safe? Professor Stupples explains: "We've started working with Airbus and Cranfield University and what we're doing is not looking at

how we can protect a system from a cyberattack – because I think a great many of the controls are already in place and it's debatable how much more secure we can get – but looking at cybersafety, which is something quite different. "If there's malware on the system – and we're talking about any system, whether it's aircraft, trains or nuclear power stations – the system needs to recognise it's behaving in an irrational manner and then revert to a safe state."

Professor Stupples gives the recent example of the Germanwings air tragedy, in which the co-pilot appeared deliberately to crash the plane. "The aircraft started to dive into a controlled but deep descent in an area with no landing facilities," he says. "The system [if a proposed failsafe was in place] would recognise this is an unsafe situation and the aircraft would then take itself to a stable state. We're looking at whether it's possible to take any system affected by malware to a safe state." It's still early days for this research. But in such an increasingly connected world, a security system that detects abnormalities would be highly valued, particularly when the consequences of malware could be catastrophic.

The all-seeing radar

Another threat to the aviation industry comes from drones. Widely available for just a few hundred pounds, remote-controlled aircraft have become a popular gadget. Although relatively small, when willingly or accidentally misused in public spaces they can potentially cause harm. More ominously, they can be armed with cameras, transmitters or even explosives and flown into controlled areas unnoticed. They could be used by terrorists for reconnaissance or flown into a descending passenger plane. There is also concern they may interfere with aircraft navigation or train controls.

Due to their size, drones often can't be seen by conventional scanning radar, so for Professor Stupples' latest research he's working with

Cambridge-based company Aveillant to develop a new kind of radar. This collaboration has led to what Aveillant calls "the world's first 3D holographic radar system". What makes this so unique is that it's able to 'look' in all directions at once, rather than be on target once every few seconds. As a result it can pick up the tiny drones.

While this advancement may be good news for the likes of Airbus, Professor Stupples says that it could have ramifications for the world's most expensive plane: the multibillion-dollar F-35 Lightning II stealth fighter. Professor Stupples says: "I believe this new radar will be able to see it, which makes you question whether [the F-35 is] the correct route to go down. Not only me but a lot of other people in the radar world take the view that this is not money well spent."

The US and UK governments, who have nailed their colours to the mast of the F-35, would probably beg to differ. Regardless, Professor Stupples' research raises an important issue.

Undoubtedly, we are living in a world where increasing digitisation and interconnectivity are bringing us many advantages. But with those benefits come new risks. Thanks to academics such as Professor Stupples and others at City, we are able to understand those risks better and introduce measures that will protect us all.

Provided by City University London