If airlines offer in-flight Wi-Fi, they should invest in an extra black box for security

April 22 2015, by Yijun Yu And Andrew Smith

Hackers in seat 61? Not what passengers want to see in-flight. Credit: Reddit

In-flight Wi-Fi is one of the most sought-after facilities for air travellers these days, now that laptops and smartphones are so common and so much of our working and personal life revolves around online services.

But a US Government Accountability Office report has suggested that many in-flight wireless networks could expose the plane to being hacked

or remotely controlled. In fact it's of such a concern to US authorities that when a well-known computer security expert made an admittedly ill-thought-out joke about doing so on Twitter, he was promptly arrested, his computers confiscated, and subsequently banned from the airline.

And all he was suggesting was to make the oxygen masks drop down. So it would appear that the stuff of Hollywood may jump from fiction to fact: Liam Neeson and Julianne Moore starred in the 2014 film Non-Stop, where a passenger hacking the aircraft's internal wireless network was entwined into the plot-based peril.

> Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone ? :)
>
> — Chris Roberts (@Sidragon1) April 15, 2015

Networks are already there

Let's step back in time for a moment: those who've had the privilege of enjoying the in-flight entertainment delivered from the back of the headrest in front of yours may not be aware that the films and music available is delivered in broadly similar fashion to that used by digital television services like Netflix and Amazon Prime.

This means that at around 30,000ft there is a computer network plumbed into every seat on board the aircraft, with a server running alongside it delivering the requested content to each user. The notion of adding wireless capability to this existing network and making the last hop to the internet proper via the aircraft's satellite communication equipment isn't a great scientific leap. The challenge has always been cost, more than concerns regarding security: satellite bandwidth is slim and expensive.

What is a surprise is the possibility that the same internet network for delivering films could also be used to control the aircraft. This is clearly not the case for all makes and models of aircraft, but it would seem that the US Federal Aviation Authority at least feel there's a risk.

Separation of powers is key

Any junior network technician knows that when you create a network, firewalls may filter traffic and intelligently monitor what passes through them, but they can be deceived. There are many pieces of software that can be easily found and downloaded that can tunnel network streams through firewalls by disguising a blocked type of content stream as another that's allowed. There are many layers of security, but equally there are also many tools that can be used to counteract them, when used by someone with the right knowledge.

In fact, it seems the authorities have rather given the game away – effectively declaring that this is a problem and that aircraft are vulnerable. Which ones, no one knows, yet – but if nothing else hackers love a challenge, and less noble-minded souls could easily do their homework to find out. How many other international security and aviation agencies are pleased with this?

Back on the ground in a traditional network, managers monitor their systems. These are not 100% foolproof nor hack-proof, which is why we have systems that alert us to potential threats and knowledgeable security experts who can interpret the data and react accordingly.

In the air, the system has to run under the assumption that there is no ability for any remote intervention of an engineer on the ground. This means that if the in-flight system is compromised there may be nothing that can be done about it. If Wi-Fi is to be provided by the airlines to their customers, the aircraft's control systems must categorically be

entirely separated from any network that passengers could access.

Record and analyse

While we're no fans of surveillance, in this instance we'd consider going one step further. If wireless networks for passengers are to be used on aircraft they should be logged, with all passenger network traffic copied into an additional black box flight recorder. Filters could flag any interesting, dubious or dangerous traffic to be passed on to an expert team on the ground via a satellite uplink, with bandwidth reserved for a compressed stream sharing this as well as other essential data regarding the flight.

This would enable a security analyst to share any concerns they may have with air traffic control, the pilots and any other appropriate authorities. These days not only do we know where the aircraft is, experts may also have a view of what is happening in the cabin.

Convenience brings problems that must be catered for: if we want the freedom of sending emails mid-Atlantic, we must first look to the safety of the flight and its crucial systems. Otherwise, no Wi-Fi is far better than having someone else flying the plane.

Source: The Conversation