The threat of cyber attacks on airlines is an issue affecting aircraft and their avionics systems, the EFB/ETL ecosystem, connectivity systems, airline IT systems and air traffic control. The nature of cyber threats and the initial steps taken to thwart them are discussed.

Addressing the issue of cyber attacks

Airlines and aircraft operators have benefitted from the steady evolution of technology used in flight controls and communications over the past 40 years. While each step of this evolution has delivered cost reductions and gains in efficiency, cyber attacks have become a steadily growing problem. The issue of cyber security was at first in the background and most were unaware of it, but concerns over cyber threats have grown to the point that airlines are now forming cyber teams, and aircraft avionic and IT system and connectivity suppliers are all having to build resistance and cyber protection into their products.

Aircraft development

There are several ways that aircraft and airlines can be exposed to or become victims of cyber threats. These include the aircraft's flight controls and computer systems, the electronic flight bag (EFB) and its ecosystem, the various connectivity systems for the flightdeck and the passenger cabin, air traffic control (ATC) systems, and airline IT systems.

While these are generally five separate issues, the growing use by airlines of the Internet of Things (IoT), e-Enablement, and big data analytics further increases the possibility of cyber threats.

"Cyber security was not an issue with first and early generation jetliners," says Brian Tighe, national training committee deputy chairman of the Allied Pilots Association. "Flight controls in early aircraft types were operated by under-floor mechanical cables connected to pilots' control yokes, which opened and closed valves on hydraulic servos. These physical flight controls, even with an electronic autopilot with selections made by the pilots, meant that the pilots were effectively the brain of the aircraft. Pilots ultimately made all the decisions and control inputs. If the autopilot failed, the aircraft could be flown manually.

"In addition to the architecture of flight controls, all communications to and from the aircraft were by voice over radio," continues Tighe. "These two main design factors meant that the aircraft was completely autonomous, and therefore not vulnerable to a cyber attack, or being 'hacked'.

"Further generation aircraft introduced in the 1970s and early 1980s were fitted or retrofitted with flight management computers (FMCs) or flight management systems (FMSs)," continues Tighe. "These aircraft allowed pilots and flight engineers to perform complex calculations and navigation functions, but the aircraft were remained autonomous and immune from cyber threats."

The two main threats to aircraft were the failing of the autopilot computer, and a physical threat from a terrorist. A problem with the autopilot computer or a failure with a part of the flight control system, such as the autotrim, meant the pilot could still fly the aircraft manually. This is reflected by the aircraft of this generation, such as the 767, requiring two electrical generators.

Data communications to and from aircraft were first introduced in the late 1970s with analogue aircraft communications addressing and reporting system (ACARS) messages. These ACARS messages were effectively a simple text messaging system. Messages were sent in a particular ARINC format that an avionic unit on the aircraft, such as the air traffic service unit (ATSU), could decipher. Conversely, an avionic unit such as the FMC/FMS could send an ACARS message to the ground via the ATSU. The message was then relayed to airline offices and departments via the networks of the ACARS service providers, ARINC and SITA.

Despite this first generation of connectivity between the flightdeck and the ground, this development posed no risk of cyber threats. Analogue ACARS messages were later joined, however, by digital ACARS messages. These allow a wider range and larger quantity of information to be transmitted to and from the aircraft. They are still channelled through the service providers' networks.

Digital ACARS messages were first used to send and receive relatively small quantities of data and information. The number of types of digital ACARS messages has steadily increased to include: automatic terminal information service (ATIS) messages; flight plans and fuel upload data and information; EFB transmissions; and aircraft health monitoring (AHM) and engine health monitoring (EHM) data. They may also include ETL and live weather information transmissions.

There has also been the development of controller-pilot data link communication (CPDLC) messages to and from the aircraft. This was first for the future air navigation system (FANS) for an increasing number of trans-Oceanic and long-haul markets in the world. CPDLC was later included as an element of the SESAR air traffic management system in Europe, and will also be used in the NextGen system in North America.

These have all become possible because of digital ACARS tranmissions over radio and satcom connectivity links.

Data transmissions have also grown with the addition of flightdeck connectivity systems with larger

Cyber threats are an issue concerning airline IT systems, the aircraft and its avionics, air traffic control, and the EFB/ETL ecosystem.

transmission capacities, such as on-ground cellular and WiFi transmissions for flight operations quality assurance (FOQA) data, and wireless software updates. Electronic manual pages and software are now updated wirelessly on the ground with many aircraft types.

Flight controls

In addition to the change and increase in the number of flightdeck transmission categories, the architecture and philosophy of flight control system design has evolved. The first major change was in the 1980s with the A320, the first commercial aircraft with a fly-by-wire (FBW) flight control system. This involved computers, using a large number of algorithms and data inputs from various avionic units, to make complex calculations and sending instructions via electrical wiring to flight control servo motors to initiate the movement of flight control surfaces.

"While the benefits of an FBW control system include the fact that it weighs less and needs less maintenance than a conventional flight control system, there are also several disadvantages," says Tighe. "The first is that mechanical cables and the physical connection between the pilot's control column and flight control servo motors has been removed. This means that a pilot is less able to control the aircraft manually if a part of the FBW system fails. The second is that the system uses digital data, so it is vulnerable to a cyber attack.

"A possible development in flight controls is the adoption of fly-by-WiFi flight control systems," continues Tighe. "This involves sending signals to flight control servo motors wirelessly from the flight control computers. Such a system would save further weight, but it would make the aircraft more vulnerable to cyber attack, however, since the WiFi signals within the aircraft could be interfered with by an outside source. Overall, the flight control system computers make the aircraft open to cyber threats."

Tighe explains that the pilot is unable to do anything on a modern generation aircraft if a digital computer fails. The situation can only be avoided if there are several back-up computers. "This means that more than one back-up computer is required," says Tighe. "The problem is that if there are just two computers, it will not be possible to tell which one is malfunctioning. Several computers are therefore required, and the system has to be able to determine which one is malfunctioning so that it can be isolated while the remainder continue to function. This has to be factored into the aircraft's avionic design and architecture. It is because of the possible failure of systems and computers that the 787 has six electrical power generators."

The issue of malicious intent also has to considered. That is, a hacker could inject a virus into the aircraft's avionic systems. This scenario is relatively easy to conceive given that data is regularly downloaded from and uploaded to modern aircraft.

In the event that one computer no longer makes sense, because it has been infected by a virus, then the remaining computers need to be able to continue to operate. This also has to be factored into the avionic architecture. "A hacker only needs to find a way into the aircraft, for example via ETL or EFB transmissions, or through software or electronic manual updates," says Tighe. "The flight control software could also be damaged when performing a regular update or revision. The implications of this are that software has to be verified as not damaged before being uploaded to the aircraft."

The cost of maintaining cyber security will therefore be a growing problem. Another big problem is that there are hundreds of possible ways to hack into an aircraft or an airline's system. There will therefore need to be an equal number of solutions.

Modern operations

There are several negative consequences of increased automation and aircraft connectivity. The development and advent of further flightdeck connectivity systems, including satcom connections, has stimulated the adoption of EFB systems. Many of these are based in commercial off-the-shelf (COTS) devices. These include a variety of tablets that are available for public purchase. Their adoption has increased the speed of concern about cyber threats. Now that COTS devices are widely being used, and it is easy to determine how they function, it has become relatively easy for the ill-intentioned to hack into them, and the overall EFB ecosystem, to cause some damage.

Besides connectivity systems, flight control system design architecture, and EFB ecosystems, there are other issues that add to the cyber security threat. These include the fact that anyone can now go on to the internet to find out about the structure and format of CPDLC messages, or acquire the wiring diagrams for aircraft avionic electronics and avionic units for a variety of aircraft types. This creates the possibility that someone could develop a system to send counterfeit CPDLC messages to aircraft, or feed false content into the navigation database of an FMS/FMC device.

It is possible for a sub-contractor that is three companies removed from an airline to put rogue data into a FMS/FMC database. The supply chain is therefore also a possible route for a hacker to exploit.

These possibilities have to be considered in detail. The issue of the EFB ecosystem reveals examples of how it is open to possible cyber attacks. One of

Rockwell Collins is one company that has devised a system to monitor the voice and data transmissions to and from all aircraft on a 24/7 basis.

these examples is that a hacker may be able to upload a counterfeit flight plan or fuel upload data that is transmitted wirelessly to the aircraft and EFB.

Besides the flight plan and fuel upload, there are many other types of data fed to the EFB through connectivity channels. There are therefore several hundred ways that an ecosystem could potentially be open to a cyber attack.

Another major issue is the increased use of internet protocol (I.P.) in aircraft avionics and flightdeck and passenger cabin communications. This is especially the case with modern aircraft types like the 777, A380, A350 and 787 that use a single avionics platform. This is referred to as an on-board network server (ONS) on Boeing aircraft and FlySmart with Airbus on Airbus aircraft.

Although these avionic platforms are using I.P., there are still three independent domains for aircraft data: the avionics; the AOA messages and communications; and passenger data. Despite a lot of conjecture and rumour, these three domains are separate and firewalled, so they are totally independent of each other. This is contrary to a United Airlines' passenger's claim that an aircraft's onboard systems were hackable. The flightdeck is in fact autonomous from the passenger cabin. There are, however, many ways that a hacker could pose a cyber threat, and each has to be considered."

Security of data transfer is now as important as aircraft and flight safety. "Networks are growing, so threats to cyber security require protection 24/7," says Joel Otto, vice president of strategy development and technology at Rockwell Collins. "Clearly Rockwell Collins operates a flightdeck connectivity service via VHF and HF radio, and via satellite communications (satcoms). These satcom systems include swiftbroadband, Iridium NEXT and u-band. All of these systems are now being used to carry some form of operations data to and from the aircraft, and they all need cyber protection."

Rockwell Collins acquired ARINC in 2014. The ARINC global network is the system over which all airline operational and flightdeck messages are transmitted. "This network is actively monitored 24/7, so that technical problems with the system can be detected and dealt with in short order. The industry is now starting to follow similar procedures for cyber threats as it does for safety threats. This includes monitoring on the aircraft, and involves the human loop factor. Moreover, no aircraft-to-ground flight operations communications go over a public network."

Areas of concern

Besides actual hacking and successful cyber attacks, the other main concern of cyber security is the doubt and fear that an attempted, suspected or unsuccessful cyber attack would create among an airline's staff and its operation. This could have further-reaching negative consequences if such an event became public knowledge.

An example is a rogue CPDLC message being sent to an aircraft. CPDLC messages are used in various air traffic management applications. These include the future navigations system (FANS) for long-haul operations, the SESAR system in Europe, and the NextGen system in the US. A hacker could potentially create a device to send rogue messages. All CPDLC messages received by an aircraft have to be acknowledged by the crew by replying to the ATC controller. The ATC controller would therefore realise that a rogue message had been sent, since it would not have sent the initial message to the aircraft. While no damage would have been done, such an event would cause nervousness to spread among flight crews. One response would be for crews to revert to using voice calls, but it would disrupt the air traffic management system. Such a scenario illustrates the need for airlines to have a second mode of operation that can be immediately adopted. This further means that pilots have to be regularly trained to use second modes of operation in the event of the failure of the first mode.

Overall, a range of security measures will have to be introduced into the EFB ecosystem, even for rogue messages that are not actually harmful to the aircraft.

Cyber threats are not posed from individual hackers only. "All possible sources of cyber threats have to be considered," says Vinnie Duggall, chief information security officer at Intelsat. "Cyber threats are possible from nation states, for-profit organisations, and even certain social groups or individuals that are trying to create some level of awareness.

"Hackers use a variety of techniques. Nation states tend to go after commercial entities in an attempt to acquire intellectual property," continues Duggall. "This can include information from defence contractors, technical data from satellite companies, and also financial information."

Cyber protection

There are now several examples of security measures being introduced to airlines' operations to counter cyber threats.

"Every component in a communication and transmission system has to be looked at," says Duggall. "This process becomes part of the selection criteria when designing, developing and building a new satellite system, for example. This includes the partners of the main satellite company, for example the companies that build the associated components such as the antenna and other parts. It therefore requires lots of cooperation."

In the case of communications to and

from the aircraft, the first barrier to cyber threats is the humans involved on the flightdeck and in the ATC systems. "It is obvious to a pilot or controller if the person he or she is hearing is a legitimate person, or a rogue individual," says Otto. "Pilots will be able to tell if a message is genuine or not, and if they execute a manoeuvre which has not come from a legitimate source, the genuine controller will also know, and be able to communicate with the aircraft.

"The same applies to fake ACARS messages," continues Otto. "Even though it is possible for someone to build a machine to generate and transmit fake ACARS messages, an ATC controller will be able to see if the aircraft is moving or changing altitude when they have not been instructed to, and so contact the aircraft."

Another issue is if a greater volume of I.P. transmissions is being sent to and from aircraft. It is possible to use encryption for these data tranmissions. This may or may not be necessary, depending on the type of information being transmitted. "The point at which encryption needs to be introduced also has to be considered," says Otto.

Two particular areas of vulnerability are the secure transfer of large volumes of AHM, EHM and FOQA data from the aircraft post-flight, and the security of the EFB network and ecosystem.

Teledyne Controls has implemented protection systems in these two areas.

Wireless data security

"With respect to data downloads, a large number of aircraft transfer data to ground stations wirelessly via cellular networks post-flight," says Murray Skelton, director of business development at Teledyne Controls. "This sends the data to an I.P. address, and the data is transferred via a public cellular network. This makes the data vulnerable to hacking.

"Following the best practice for data security is extremely important," continues Skelton. An alternative to transferring data to an I.P. address via a public network is for an airline to move away from this industry standard," continues Skelton. "The first step is to encrypt the data using a Teledyne encryption. The data can then be transferred via a virtual private network (VPN). This is a hidden data tunnel between the aircraft and ground receiver that is not a public cellular data pipe, which means that it is secure.

"Even if it is discovered, the VPN requires authentification," says Skelton. "We have chosen a Spec 42 certificate for this. Spec 42 determines how the certificate gets handled and used. The certificate is agnostic to the data transfer system used. For example, ACARS data messages over an I.P. connectivity pipe can now get transmitted to the ground without being heard over regular radio and aircraft connectivity equipment.

"The certificates protect the VPN first by a username and password. These will make the VPN difficult to hack into especially if the username and password are frequently changed," continues Skelton. "Moreover, once the VPN tunnel has been established, there are two secure keys, one at either end of the tunnel. These keys are made of thousands of characters to encrypt the username and password and they are identical. These codes have to be changed frequently to stay ahead of the hackers."

Skelton confirms that a VPN is a secure way to connect two wireless devices. The three main issues for this security are that the data in the VPN tunnel is encrypted, that the keys are encrypted, and that the data is not being sent down a public network. The Teledyne Ground Comm + system can now connect through an aircraft Ku-band satellite communication system. The data is sent through a secure tunnel, so it is kept separate from the in-flight entertainment (IFE) data communications.

Several aerospace and software vendors have developed security and data encryption systems for the information passed between the aircraft and centres such as air traffic control and airline operations departments.

EFB security

EFB security can be achieved in several ways. One method is to stop foreign devices joining an airline's EFB network and ecosystem, and also the aircraft's connectivity ecosystem.

"Most EFBs are standalone devices, and they can wirelessly receive data from an aircraft's systems and avionic units for the pilots to then perform calculations. Data is not sent from a standalone EFB to the aircraft's avionics," says Skelton. "This transfer of data and information can give a hacker the opportunity to break into the wireless connection, and possibly send rogue data to the EFB.

"This can be prevented through the provision of digital certificates to each EFB unit and each aircraft in the fleet. These digital certificates recognise each other. Devices that do not have a recognised certificate will not be allowed to connect to the network," continues Skelton. "Digital certificates are placed on each EFB device and on each aircraft. As EFB tablets are often provided to each pilot, and each aircraft will be flown by a large number of different pilots, the digital certificates on the aircraft have to be able to recognise the certificate on every EFB used by pilots that are ever likely to operate the aircraft. The digital certificates have to be changed regularly to stay ahead of hackers.

"The digital certificates are managed electronically and remotely, and are sent to the aircraft via devices wirelessly," continues Skelton. "The digital certificate technology is called Radius. The certificates can be changed manually or by Airwatch. The Radius authentication server requires that every EFB device and the aircraft all have a certificate to allow them to connect into the EFB ecosystem. Moreover, only a limited number of devices is permitted in the ecosystem.

"The security system also has a monitoring and reporting element, and this follows and monitors all the individuals that attempt to connect to the ecosystem, and who actually make a successful connection," says Skelton. "The monitoring system follows all the relevant information, including the computer I.P. addresses of the people trying to connect, or actually connecting to the system."

This EFB security system has been implemented, and it will soon get its supplemental type certificate (STC). It has the same security as data transfer systems on the ground.

Avionics security

In addition to the EFB ecosystem and wireless connectivity systems, security and protective systems have been developed for avionic units on the aircraft. Razor Secure in the UK builds software that resides on existing hosts, such as an aircraft's avionics server, to host cyber intrusion detection and prevention systems. "The software is used to detect abnormal communications and transmissions, and so creates an alert," says Lewis Oaten, chief technology officer at Razor Secure. "The system is autonomous in that it does not rely on connection with another server. The software could be hosted on the aircraft's ATSU, for example. This compares to traditional detection systems that rely on a constant connection to the internet to process data and create an alert. In the case of the ATSU, the alert is given to the pilot when the aircraft is in the air, or the alert is sent to the operations department when the aircraft is on the ground. The satcom system could be used to send the alert."

The Razor Secure system can also pick up early scanning, as is the case when a hacker is planning an attack and is trying to work out how a system works.

Cyber security community

Aviation ISAC was established in September 2014 to strengthen and accelerate the ability to identify, prevent, detect, and respond to vulnerabilities and threats. "Aviation IDAC has been created to provide a means for collaboration across the airline, air transport and commercial aerospace industries to generate and nurture trusted relationships for cooperation in cyber threats and security," says Jeff Troy, executive director at Aviation ISAC. "The organisation now has 27 member companies from five continents.

"The philosophy behind the organisation is that an airline can control its own systems, but it cannot help an airport, ATC, other airlines, or connectivity system providers in the event of a cyber attack," continues Troy. "That is, all companies and individual organisations are on their own. Aviation ISAC provides a forum where understanding and intelligence on cyber threats and security can be shared. The overall objective is to build resilience for aviation."

One goal behind Aviation ISAC is to create a safe environment where all members of the organisation can share information with other members through trusted relationships. If there were an attack on a part of the industry, then through Aviation ISAC the members would have access to all the cyber analysts available. The forum also helps its members fully use all the intelligence that has been gathered by the community to deal with the threat, by gathering and . developing the skills to spot, detect and gain the necessary forensic evidence. Aviation ISAC also sends regular reports to members to help them improve their cyber security. - *CHW* AC