IFALPA
The Global Voice of Pilots

Position

14POS03 5 June 2013

Cyber threats: who controls your aircraft?

Background

The IFALPA Security Committee has identified the possibility of a cyber attack against an aircraft, ground facility, or other critical infrastructure to be a significant and emerging threat. The purpose of this paper is to articulate this threat, and suggest ways in which it might be addressed.

General

- The typical commercial flight operation, whether passenger or cargo, generates and requires a large amount of data. This data is used not only for the normal operation of the aircraft, but can also be utilized to provide support and comfort functions for crews and passengers alike. Operators, air traffic service providers and manufacturers amass a great deal of sensitive and even confidential data on their employees and passengers. This data is normally stored on computers and transmitted across networks to other computers; this transfer of data is, in fact, critical and integral to the operation of a modern commercial aircraft.
- Much of this technology is not new, and was in fact developed at a time when its security was not a key factor. But it is a fact that the safety of the flight relies heavily on proper information. Therefore, it is important that personal data of passengers and crews have to be protected against misuse.
- Cyber attacks in society in general are on the increase and are in fact very frequent. They can be carried out from virtually anywhere by anyone with sufficient knowledge, using low-budget methodologies. The goal of these attacks is to obtain confidential, critical or sensitive information, to manipulate or erase information and/or to control or destroy systems or services. We have seen that in many cases the compromised system may have not even been targeted but is taken down as a result of an attack elsewhere; in other words, it is a victim of "collateral damage".
- Therefore security should be considered throughout all communications pathways and applications. As with anything, the system will only be as strong as its weakest component. An effective defensive system is one that provides for the fact that if one component fails, another will take its place.
- This security should protect data through its entire lifespan, from initial creation to final disposal. The information should be protected not only when in motion (i.e. while traveling on a network), but when at rest as well.

Software

- Providers of software (including firmware) and operating systems should be able to demonstrate adequate security measures that have the ability to protect from both without and within. Vendors of these systems must provide updates on a regular basis and additional updates that resolve security issues shortly after they have become known.
- In addition, applications should be demonstrated to function only in their intended manner. Commercially available "off-the-shelf" applications should be avoided, as they are more easily subject to security issues. Both operating systems and applications need to be designed to be highly resistant to unexpected conditions or unwanted actions initiated by users or by malicious software. Diversification of operating systems may reduce vulnerability.
- Running of applications within individual so-called "sandboxes" (virtual protection zones) limits unwanted interaction of software. Anti-virus software needs to be applied and it should be updated as required. Backups need to be performed on a regular basis and stored separately (i.e. without a physical connection to a network).

Hardware

- Hardware providers need to demonstrate the effectiveness of security measures against cyber attacks from both within and without. If commercially available, off-the-shelf hardware is used it needs to be regularly evaluated as to its vulnerability and stability. Components need to be protected against physical access.
- Storage devices need to be encrypted and secure.
- A device that is used for professional purposes should never be used for private means unless the operating system supports sandboxed application running only, and applications are from certified and trusted sources.
- Systems that do not fulfill security and safety requirements should never be connected to secure systems without further security measures taking place.
- Highly sensitive systems should be physically separated from the Internet and networks that have access to the Internet. This

includes separation of in-flight entertainment systems and their communications from all other aircraft systems.

- Facilities housing systems that store, process or send sensitive data should be considered and guarded as a security restricted area.
- Data Protection (Electronic and Physical)
- Data transfer should only take place via a secure and encrypted channel. Internet connections should be avoided if possible. Medias for data transportation should be read-only and should be destroyed when outdated. All transfer data, whether via a network or by a physical transfer, should be encrypted and secured.
- Message integrity (i.e. no undetected data modification) should be guaranteed throughout the entire transportation/transmission process. Appropriate techniques should be utilized to guarantee that data, transactions, communications, and documents are genuine, parties involved are who they claim to be and they cannot deny having sent or received a transaction.
- Access control should be at minimum a two-step barrier and should consist of two of the following things, depending upon the circumstances:
  - Something known to an individual (i.e. a password or PIN).
  - Something that one owns (i.e. a smart card or security token).
  - I biometric such as an iris scan or fingerprint.
  - One's physical location (i.e. inside or outside of a company firewall, or proximity of login location to a personal GPS device).
- Data that is classified as personal or that is relevant for the safe operation of aircraft should never be stored, processed or transferred by any system that does not meet the security and safety requirements of this policy.
- Network traffic, ACARS, and EFB communications and applications should be continuously monitored. Since the majority of cyber attacks go unnoticed for long periods of time (sometimes many months), forensic analysis should be applied to accumulated data and logs.

Training of Flight Crews

- Air operators should establish clear training guidelines for the use of, and interaction with, aircraft equipment and infrastructure that involves data usage. Such equipment includes, but is not limited to, Flight Management Systems, FANS, ACARS, CPDLC, and Electronic Flight Bags
- This training should address:
- Crew awareness of security vulnerabilities,
- How systems can be attacked,
- What precautionary measures could prevent an attack or minimize its consequences,
- What an attack might look like to an operating crew member, and
- Possible actions that may be taken should a crew suspect that their aircraft or any other part of the aviation infrastructure may have been the victim of a cyber attack, including appropriate contingency procedures and mandatory reporting of all suspicious computer-related occurrences and malfunctions which could be related to a cyber attack,
- Crew awareness of the fact that sensitive data might be sought or gleaned from social networking sites.

Governance and Control

- Security policies and procedures should be established. Roles, responsibilities, and segregation of duties have to be defined enterprise wide. All employees in the organization, as well as business partners, should understand the reasons for restrictions of access to data and the steps required for individuals to be granted this access, and understand the required security controls and handling procedures.
- An Information Security Management System (ISMS) should be established, defining a system of processes, together with the identification and interactions of these processes, and their management. The ISMS should include a "Plan-Do-Check-Act" model to ensure that the required level of security is maintained at all times. Attention should be given to three specific areas:
- GRC (Policies, Governance, Risk, Compliance)
- Visibility (Monitoring, Analytics, Incident Management)
- Controls (Security solutions for secure access, encryption, firewalls, network IPs, host and workstation IPs, DLP, etc.)
- As part of an ISMS system, all operators, air traffic service providers and manufacturers should be required to designate an individual to serve as a "single point of responsibility". This person would be the "accountable executive" who would be responsible for their information security policy and procedures and its governance.
- Within the ISMS an information security risk management process should be established. Risk assessments of both the own organization and external data providers should be made, to ensure the required level of assurance is provided.

- ISO standards 27001 to 27005 provide detailed guidance in establishing and implementing such an ISMS.
- National legislators should regard all kinds of cyber attacks towards aviation and its infrastructure as very serious and dangerous acts, and should criminalize them accordingly.

Air Traffic Services

- Navigation data is currently provided in a non-secure form. Corruption of this data could conceivably lead to serious navigation errors. There may be a need for systems capable of monitoring, crosschecking, and verifying the veracity of this data. There are many communications bands available that might require integration (i.e. different bands on satellite frequencies) but the data must be usable for the required navigation, surveillance and/or communications functions.
- It is noted that under Attachment B to ICAO State Letter ST 13/1 – 11/71, reference is made to the integration, interoperability and harmonization of systems in support of the "One Sky" concept for international civil aviation. Specific reference is made to "High-level impediments to implementation such as cyber security should be identified and considered as part of the roadmap development process". ICAO is therefore taking this issue very seriously.
- ACARS systems are also notoriously unsecure. It should be noted that the ACARS systems are a carrier-specific system in the public domain, and was not designed for ATC communications or other critical messages. However, some States have laws prohibiting the transmission of personal information over such systems. These States now encrypt ACARS communications. We do see, however, a move by some States toward active discussion of the feasibility of using ACARS systems for limited CPDLC (Controller-Pilot Data Link Communications).
- The physical security of ATS facilities also needs to be addressed. Just as IFALPA has advocated for identity verification and vetting as the preferred and most effective method of screening pilots entering the secure area of the airport, we also see a need to ensure that individuals allowed access to ATS facilities both at and away from the airport must be fully trusted and have strict access controls, preferably using biometric access protocols, in place. In addition, much more attention should be given to physical barriers around such facilities.
- There are many methods to protect signals that we rely on to effect communications, navigation, and surveillance functions. Most are based on technologies and may be adapted from military methods, such as encrypting VHF transmissions. The proposals to provide more secure links would need to be simple to deploy and execute, while being universal or at least harmonized. Robust measures should be put into place to prevent unauthorized individuals from accessing ADS-B uplink and downlink messages, secure and reliable GNSS signals, and securing the controller-pilot data link communications. A complete systemic risk assessment in order to analyze the actual threat for all Communication-Navigation-Surveillance (CNS) systems is required.

Aircraft Design and Operation

- Methodologies that may address vulnerabilities of civilian GPS signals need to be explored, such as the recent inclusion of the L5 signal; however, this may not address malicious intent. Further study is also required to determine the level that the Fault Detection and Exclusion (FDE) protocol within GPS receiver systems may mitigate malicious interference attempts, and if so to what extent.
- It is important to note that encryption systems that might be applied to navigation data (GNSS, etc.) should not impair the transmission of such data or slow the data processing down. Additionally, FMS units and EFBs should be encrypted by different algorithms in order to protect against encryption-enforced errors. Thus, two sets of data would be created for normal use.
- The possible inclusion of a "security code" or some other such protocol, known only to authorized senders and receivers, may mitigate the inherent vulnerability of ACARS systems.
- Although it would be a challenge to corrupt ACARS received data with any high degree of success, "annoyance spoofing" (i.e. corruption of the genuine signal) should be addressed.
- The integrity of ACARS data could be enhanced by encryption, but it should be considered that the "key" would need to be protected and changed on each sector. Transmission of the public key segment should be passed by a secure means other than ACARS.
- The use of a multi-layered system that would prevent unauthorized personnel physical access to aircraft, as well as security procedures designed to "look for things that don't belong", may prove to be the most effective way to ensure the physical security of the aircraft.