Modern approach to cybersecurity of computer-integrated aviation systems

A V Ilyenko[1,2], S S Ilyenko[1] and D S Kvasha[1]

[1] Information Security Systems Department, National Aviation University, 1 Liubomyra Huzara ave., Kyiv 03058, Ukraine

[2] E-mail: ilyenko.a.v@nau.edu.ua

Abstract. Considering computer-integrated aviation systems that provide a link between civil aviation activities within the "ground-to-air" and "air-to-air" channels, the question of the safe operation of such aviation systems from an ever-increasing cyber threats, and the decline in cybersecurity for the aviation industry as a whole. The protection status of "ground-to-air" and "air-to-air" channels in such aviation systems is at different levels and depends directly on the activity of all components of aviation activity (airport-aircraft-information network-air traffic management, etc.). In view of the ever-increasing cyber statistics on the work of civil aviation worldwide, the authors of the article highlighted the current state of cyber security and protection of "ground-to-air" and "air-to-air" channels of the aircraft fleet of Ukrainian airlines, and take a closer look at the world experience. The authors comprehensively covered all components of the aviation system, with particular attention given to aircraft designed by Antonov Design Bureau with the time evolution of tire development and data networks of the world's leading aviation industry leaders (such as Airbus and Boeing). Also, attention is given to the present state and mechanisms of data transmission of the "ground-to-air" and "air-to-air" channels and the architecture of the modern air-network of computer-integrated aviation systems.

1. Introduction

The secure exchange of information in today's realities is of growing concern to users around the world. Basic data that is transmitted openly is vulnerable to a variety of cyber-attacks that can threaten the integrity and accessibility of any information system that aims to ensure the transmission of important critical information. There is concern that without the use of robust cybersecurity research, critical systems that humans rely on may be prone to cyber-attacks. The urgency of cyber security in the aviation industry has been exacerbated by the widespread use of the Internet and wireless communication in information transmission systems between the methods of communication of airport control points, aircraft and air navigation systems to ensure and control air traffic along the flight route system based on the information network "Ground-to-Ground", "Ground-to-Air" and "Air-to-Air". Such systems are commonly referred to as computer-integrated aviation systems. Ukraine as part of the aviation community with its aircraft construction component (SE "Antonov") must move in unison with leading manufacturers and operators of aircraft. From the practice of using information technology of leading global manufacturers (Boeing, Airbus, etc.) in modern aircraft over the past decade began to implement effective methods of protection and counteraction to cyber threats in the

transmission, storage and processing of critical flight data. One such example in the field of aviation is reliable identification methods between aircraft and air traffic control systems. Considering the computer-integrated aviation systems described above, we can see that it contains a large amount of critical information that has a confidential status, so if the information is transmitted openly, these systems become quite vulnerable to cyberattacks. Threats and risks will increase with the increase of connected information transmission devices both in the airport information networks and in the networks of the aircraft directly. This can lead to the launch and spread of various cyber-attacks. Therefore, cyberattacks in the aviation industry can threaten both the safe operation of the aircraft itself and the aviation system as a whole (on a scale within the state and interstate air services).

In view of this, it is necessary to introduce and use a number of means to protect the integrity, confidentiality of information in aviation systems for transmission, storage and processing of important critical data. Using modern technology, aviation systems for transmitting, storing and processing critical data are becoming increasingly automated and can work both in pairs and independently of the voice commands of air traffic controllers. Relevant avionics systems of modern aircraft can now broadcast and receive information about the aircraft and its location using transponder technology. This reduces the load on control points along the entire flight route and allows the aircraft to take more responsibility for maintaining flight safety. However, these aviation systems lack methods to authenticate the source or the ability to verify the integrity of the content of the information message. This opens the possibility for hackers to potentially create fraudulent information messages or manipulate the content of messages, which, in turn, can affect the controls of the aircraft in the "autopilot" mode and divert it from the specified flight course. Careful research in the field of aviation data transmission makes it possible to clearly understand the primitives of cyber security in order to form a reliable security project to protect aircraft from cyber threats in general. Articles [1] and [2] highlight the main problems and challenges facing the aviation industry worldwide, and articles [3-9] identify the main areas of protection of "ground-to-air" communication channels. The *purpose* of this work is to study the current state of information security in the aviation industry of Ukraine, which allows to analyze the main problems and highlight the main ideas of the authors to solve them.

2. Theoretical fundamentals of research

Characteristics of threats of aviation communication channels. On-board wired and wireless avionics devices of the aircraft have access to the system of construction of routes of air routes and to program algorithms of flight on the route with the help of aircraft controls in different flight modes (modern on-board computer FMC-Flight Management Computer which is controlled by display CDU - Central Display Unit). Unauthorized reprogramming of the route (including hacking methods) can lead to intentional or unintentional damage to data and / or systems that are important (critical) for the safe operation of the aircraft. Threats also exist for the operation of all automated functional systems (FS) and aircraft avionics complexes. Typically, critical access points are Internet access points (through the software provider to its operator or contractor) and points where programmed information is transmitted from the operator (airport or control point along the route) to the aircraft. The issue of ensuring the cyber security of the aviation industry is very relevant today, as circumstances in Ukraine and the world clearly show this.

Here are some facts of cyber-attacks in the aviation industry in the world: 2006 - internet attack on US air traffic control centers; 2008 - infection of the on-board computer of the flight Spanair 5022 with malicious software, which led to a crash; 2009 - interference with the US GPS system used to land the aircraft; 2013 - interference in the information system of airports in Turkey, which led to the suspension of passport control; 2013 - interference in the computer networks of 75 US airports; 2014 - loss of aircraft control during remote connection to autopilot and disappearance of Malaysia Airlines flight MH370 from radar (one of the key versions of the disaster); 2014 - large-scale attacks on computer aviation systems in Pakistan, Saudi Arabia, South Korea and the United States; 2015 - the spread of malicious software in the computer systems of the US airport, which led to the suspension of

flights; 2015 - unauthorized interference in the computer system of the airport of the Polish airline LOT, which led to failures in the maintenance of the aircraft and loss of confidential information; 2016 - intrusion into the computer system and infection of computers at Tallinn Airport with malicious software, which led to the loss of confidential information; 2017 - interference with the computer system of US domestic airlines, which led to the forced landing of the aircraft and the failure of the Aircraft Communications Addressing and Reporting System (ACARS); 2018 - eurocontrol's computer system crashes, disrupting the integrity of the data exchange system and delaying more than 15,000 flights in Europe.

Ukraine first suffered a cyber-attack on computer systems and the central server of "Boryspil" and "Kharkiv" airports in June 2017, resulting in denials of aircraft maintenance and delays in departures. A few months later, in October 2017, there was a delay in the departure of aircraft from the airport in Odessa as a result of hacking the computer network of the airport, which led to the loss of confidentiality of information.

According to experts from the European Aviation Safety Agency (EASA), during 2019, the world's aviation systems were subjected to cyber-attacks up to 1,000 times a month. Thus, approaches to countering cyber-attacks should be systematic, reliable and comprehensive, the aviation industry belongs to the objects of critical transport infrastructure of Ukraine. The security program for the transmission of critical information in the relevant aircraft avionics systems must be designed to protect, reliability, integrate and secure the network and data. Effective security of the transmission of critical information in computer-integrated aviation systems is aimed at combating various threats and prevents them from entering or spreading in aircraft avionics systems. The most common threats include: viruses, Trojan horses; hacker attacks; provoking pseudo-failures during the operation of various FS and aircraft complexes when in fact the systems are in working order; interception and data theft; activities and influence of hostile intelligence, etc. A successful attack can lead to complications in the operation of the functional systems of the aircraft, the development of complications of flight conditions, and in the case of an increase in false data on flight conditions - to accidents and catastrophes. Threats can cause a variety of failures and failures, as the aircraft's aircraft are very complex and saturated with complex computer networks. As a result of the analysis of specialized literature and online sources, the authors grouped, synthesized and tabulated modern types of cyber threats in the context of modern civil aviation [3-9].

To date, the use of reliable and effective methods of protection of information transmitted in the system of interaction "ground-air" requires in-depth research, because these channels are unprotected [10,11].

Current state of data transmission in aircraft avionics systems, security and problem areas. Previously, aircraft were used in civil (ARINC 429 / ARINC 629) or military aviation (MIL-STD-1553) standard buses for data transmission in FS avionics. The information transfer processes using the TCP and / or TCP / IP transmission protocol were physically and logically isolated from the use of aircraft avionics in the FS.

Development of aviation technologies in the field of FS data transmission: ARINC 429 (100 kbit / s) - linear unidirectional bus; MIL-STD-1553B, also known as DEF-STAN-00-18 and STANAG 3838 (1 Mbps) - linear bidirectional bus with centralized control, command / response protocol; ARINC 629 (2 Mbps) - linear bidirectional bus with distributed control, with multiple access / collision recognition (CSMA / CD), as well as with dynamic time slot distribution (DTSA); ARINC 664 (AFDX Ethernet 10/100 Mbps) - bidirectional communication network with distributed control and CSMA / CD protocol to provide pseudo-determined time and redundancy management; CANbus (1 Mbps) is a linear bidirectional bus with a priority collision "detection / avoidance" protocol.

In the table 1 collected, substantiated and compared the characteristics and performance of the main information buses in the FS communication networks used in modern aircraft construction [12,13].

Each bus or data network has found its place in the architecture of the FS avionics of modern aircraft. The key requirements are to meet the requirements for productivity, integrity and affordability

(price component). ARINC 664-P7 is suitable for high bandwidth, information base for all aircraft avionics FS, including flight control and navigation, implementation of a modern "glass cabin" ergonomics interface. ARINC 429 is used as a means to communicate and check the status of the FS during diagnosis and built-in control of vital parameters. CANbus is suitable for communication with various sensors, as well as for data transmission within the FS of the aircraft.

Table 1. Comparison of data buses «Data bus network»

Bus, network	**MIL-STD-1553B**	**ARINC 429**	**ARINC A664-P7**	**CANbus**
Max. message length	32 × 16-bit	18-bit	1518 bytes (1 byte = 8 bits)	8 bytes
Max. speed	1 Mbps	100 kbps	10/100 Mbps	1 Mbps
Type of connection	Duplex Half duplex	One-way	Duplex Full duplex	Duplex Half duplex
Protocol	Command / response	Direct	CSMA / CD + extension	CSMA/CD
Max. bus length	100 m	65 m	<100 m	40 m
Signal delay	None	Insignificant	Depends on the load	Depends on the priority
Error containment	Parity bit	Parity bit	Cyclic redundancy check	Extensive cyclic redundancy check
Error handling	Feedback	No feedback	Feedback	Immediate attempt to communicate again
Reservation	Double	Simple	Double	Simple
Physical realization	Double "twisted pair"	"Twisted pair"	Double "twisted pair" or optical fibre	Twisted pair or optical fibre

World leaders Airbus and Boeing have different architectural philosophies that integrate CANbus and ARINC 429 tires with the ARINC 664-P7 network. The Avionics Standard Communications Bus was developed by Honeywell and is used in CA and business jets at a speed of 670 kbps. A commercial standard data bus developed by Rockwell Collins for use in CA, similar to the ARINC 429, runs at 12.5 kbps and 50 kbps. The RS232, RS422 and IEEE 1394 Firewire digital buses with a speed of 800 Mbps are also used in digital video transmission.

On the example of a graphic image (Fig. 1), the authors integrated and showed the technologies of data buses used in the aircraft of Ukraine in accordance with the evolutionary use and implementation of buses and data networks of world aircraft leaders [12,13].

New types of aircraft use TCP / IP technology for systems that connect both domain aircraft and cab interfaces in a way that makes the aircraft virtually a network domain server. The architecture of this air network allows you to connect to external systems and networks, such as wireless transmission systems and service systems, satellite communications (SATCOM), e-mail, the Internet and more. The main advantage of using the TCP / IP protocol is the ability to transfer information to the aircraft without the use of media. Using this approach leads to vulnerabilities and external threats, which can lead to unauthorized access and affect the work of the FS avionics aircraft. Unauthorized access to the avionics modes of the aircraft at any stage of the modern air network (the author's vision of the modern air network is shown in Fig.2) will lead to a violation of confidentiality, integrity and

availability of data, which is likely to create extreme operating conditions, substantiates the application of cyber security and security of competitive business of airlines in general.

When distributing software for aircraft avionics FS, hackers may attempt to manipulate and damage critical software designed to update the aircraft software. Under the concept of manipulation and damage to critical software will be understood as intentional unauthorized manipulation of the original software or the introduction of counterfeit software. Improper detection of software manipulation, falsification of administrative messages of the aircraft (ie download commands, requests and relevant responses) can lead, for example, to false alarms and general denial of services. This type of software attack can create unreasonable flight delays and endanger aviation safety in general. In view of the above, the transmission of critical data necessitates the development of a clear safety program for the operation of the aircraft to ensure proper control over the management / distribution of software and the security of the information network on board the aircraft.

3. Further directions of research.

Developing the concept of neurobiosensor (NBS), the author proceeded from the results of biophysical in further research, the authors plan to focus on the organization of protection of “ground-to-air” and “air-to-air” channels in experimental computer-integrated aviation systems using cryptographic methods of information protection, namely the use of asymmetric cryptography and infrastructure the public key. Asymmetric cryptography, known as public key cryptography, uses modern number theory to create two keys, one public and one private, that work together to achieve a number of cyber security goals to identify and authenticate information sources [14].

The modern engineering research approach encourages the relevant important operational implementations in the work of the studied aviation systems of the corresponding private keys. Each aircraft and air traffic control center (ATC) must use private keys with mandatory access to their public key when exchanging information. This solution allows you to encrypt the message with your private keys, and all other participants in the exchange of information have the opportunity to decrypt the corresponding public key. This approach will provide a mutual authentication and identification procedure.

Consider the theoretical approaches, namely the idea of the authors to apply the technology of “public key cryptography” for the aviation system based on the information network “ground-to-air”. A careful study of the areas of ATC and cyber security has revealed a potential problem with modern methods of aircraft identification and monitoring, as well as the tools needed to address these problems. Formal identification of the problem and the search for such potential solutions have led to the realization that the implementation of a powerful public key infrastructure is appropriate, aimed at ensuring reliable authentication and secure communication between aircraft devices and beyond. The use of PKI-based authentication will prevent communication with unauthorized components or external unauthorized devices and is aimed at eliminating a wide range of attacks. The dual path of the PKI is one of the first proposed designs for the protection of security vulnerabilities in the data communications “aircraft - aircraft” and “aircraft - ATC”.

The purpose of the PKI is to protect information (assets) transmitted or exposed to the external environment, and to protect the exchange of information between airlines in the organization of protection of “ground-to-air” and “air-to-air” channels. Hereinafter, the aviation CPI will be understood as a set of technologies and policies involved in the management, storage and revocation of end-user public key certificates in the organization of aviation communication security or in the distribution and / or use of software. The ideological construction proposed by the authors solves the problem of aircraft identification with the help of reliable methods of mutual authentication between the aircraft and the ATC. It is the dual path of the public key infrastructure that introduces modern digital signature technology, which allows aircraft to authenticate and fully protect every information message they transmit. Extensive scientific and methodological research is needed for computer-integrated aviation systems that operate directly on board the aircraft. The authors of the article are set

to comprehensively consider the problems and ways to implement the issue of cyber security of such FS in subsequent studies.

Conclusions

This article highlights the current state of cyber security and protection of “ground-to-air” and “air-to-air” channels of the park of aircraft operated by Ukrainian airlines, as well as discusses in detail the world experience in this area. The main problems of the research are analyzed, effective ways of their solution and counteraction to cyberterrorism are considered. The facts of cyber-attacks in the aviation industry in Ukraine and the world over the last decade are analyzed and presented in detail, as well as a generalized description of threats to air communication channels that violate the availability, confidentiality and integrity of information. Particular attention was paid to aircraft designed by Antonov Design Bureau, an analysis of the evolutionary development of tires and data networks of modern aircraft of the world's leading leaders Airbus and Boeing and design decisions of the State Enterprise Antonov. It is shown that the growth of cyber-attacks in civil aviation is accompanied by the introduction and application of modern information and communication technologies, which on the one hand increases efficiency, and on the other hand increases the number of vulnerabilities and opportunities for cyber impacts on computer-integrated aviation systems.

The current state of data transmission of “ground-to-air” and “air-to-air” channels is highlighted, and the architecture of a modern air network, computer-integrated aviation systems, is summarized. Based on the above, the proposed theoretical approaches to the organization of cyber security of aviation communication channels using encryption methods and approaches, namely the use of public key infrastructure to authenticate and control the integrity of messages to ensure the organization of air traffic. The team of authors plans to develop and implement effective methods and tools for further scientific and technical activities to ensure the requirements, principles and approaches to cyber security and organization of protection of “ground-to-air” and “air-to-air” channels.

References

[1] Fatigue risk management system implementation guide for operators [Online]. Available: https://www.researchgate.net/publication/312971231_Fatigue_Risk_Management_System_in_Aviation

[2] Aviation security law 2010 Ruwantissa Abeyratne [Online]. Available: https://books.google.com.ua/books?id=tw8g6C479vUC&pg=PA116&lpg=PA116&dq=aircraft+pki&source=bl&ots=JcZ_b5z7yL&sig=xlkbmLsRXTO6Y2FPNPrpZnvH52s&hl=ru&sa=X&ved=2ahUKEwjzzsb525reAhVFpYsKHbJcAMo4ChDoATABegQICRAB#v=onepage&q=aircraft%20pki&f=false

[3] Safety Management Manual [Online]. Available: https://www.skybrary.aero/bookshelf/books/644.pdf

[4] DPP: Dual Path PKI for Secure Aircraft Data Communication [Online]. Available: https://vtechworks.lib.vt.edu/bitstream/handle/10919/20373/Buchholz_AK_T_2013.pdf?sequence=1

[5] The Boeing Company Boeing Commercial Airline PKI Basic Assurance CERTIFICATE POLICY [Online]. Available: http://www.boeing.com/crl/Boeing_BCA_PKI_CP_1.4.pdf [Accessed: 22 march 2020]

[6] Aircraft Network Security Program [Online]. Available: https://www.caas.gov.sg/docs/default-source/pdf/ac121-7-2(rev-0)-aircraft-network-security-progamme-(ansp).pdf

[7] Mohamed-Slim Ben Mahmoud, Nicolas Larrieu and Alain Pirovano 2010 A performance-aware Public Key Infrastructure for next generation connected aircrafts. DASC 2010, 29th IEEE/AIAA Digital Avionics Systems Conference, Oct 2010, Salt Lake City, United States. pp 3.C.3-1 - 3.C.3-16 DOI: 10.1109/DASC.2010.5655369

[8] Robinson Richard V, Mingyan Li, Scott A Lintelman, Krishna Sampigethaya, Radha Poovendran, David von Oheimb, Jens-Uwe Buber and Jorge Cuellar 2008 Electronic

Distribution of Airplane Software and the Impact of Information Security on Airplane Safety, 4680 Springer Berlin / Heidelberg 28-39. DOI: 10.1007/978-3-540-75101-4_3

[9] Robinson Richard V, Mingyan Li, Scott A Lintelman, K Sampigethaya, Radha Poovendran, David von Oheimb and Jens-Uwe Buber 2007 Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes. DOI: 10.2514/6.2007-7769

[10] Appendix 17 to the Convention on International Civil Aviation «Security. Protection of international civil aviation from acts of unlawful interference». [Online]. Available: http://www.6pl.ru/asmap/Annexes//an17_cons_ru.pdf (in Russian)

[11] Doc 8973 ICAO «Aviation Security Manual» (Restricted) [Online]. – [Online]. Available: http://dspk.cs.gkovd.ru/library/data/8973_cons_ru_ruk__vo_po_ab_izd_9_e_2014g_.pdf (in Russian)

[12] Ian Moir, Allan Seabridge and Malcolm Jukes. Civil Avionics Systems. [Online]. Available: http://dl.booktolearn.com/ebooks2/engineering/aeronautical/9781118341803_civil_avionics_systems_fffd.pdf

[13] Ian Moir and Allan Seabridge. Aircraft Systems Mechanical, electrical, and avionics subsystems integration. [Online]. Available: https://soaneemrana.org/onewebmedia/AIRCRAFT%20SYSTEMS%20BY%20IAN%20MOIR%20&%20ALLAN%20SEABRIDGE%20TRIBIKRAM.pdf

[14] Kazmirchuk S, Ilyenko A and Ilyenko S 2020 Digital signature authentication scheme with message recovery based on the use of elliptic curves. In: Hu Z, Petoukhov S, Dychka I and He M (eds.) ICCSEEA 2019. AISC vol 938 pp 279-288. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-16621-2_26