Bilge International Journal of Science and Technology Research
Web : http://dergipark.gov.tr/bilgesci - **E-mail:** kutbilgescience@gmail.com

Received: 13.03.2018
Accepted: 23.07.2019
DOI: 10.30516/ bilgesci.405074

ISSN: 2651-401X
e-ISSN: 2651-4028
3 (2), 135-143, 2019

Air Traffic Security against Cyber Threats

Ahmet Efe [1]*, Ahmet Can Cavlan[2], Büşra Tuzlupınar[2]

Abstract: Air Traffic Management security is amongst major topics of safety of critical systems and issues of both civil aviation and military defense units. The dramatic increase in the number of the aircrafts and the innovative technology that provides smaller and sustainable air vehicles make the air communication protocols and methods as a high profile potential target for black hat hackers. There are lots of communication protocols and different systems between air to ground station and air to air. These include set of information such as aircraft communication data, voice information and flight planning which works on some protocols. All of radar detection and chasing systems are also using similar techniques including air defense and army elements. The Data Distribution Service is a protocol for data transfer to each node. Since there is not any full assurance, the communication systems can be protected from third party system or hackers to some extent. The security is coming from that point. Each components have own security using valid and standard methods. Our approach and objective in this study, is to provide reasonable and applicable security concepts and techniques for robust and resilient air traffic via a literature survey and analysis.

Keywords: Information security, DDS, ATM security, ATC, ADS-B.

1. Introduction

Hacking of aircrafts is becoming one of the most important challenges that cyber security experts are trying to find additional remedies for vulnerabilities. Portable RF transmitters used by hackers can only be operated with an easily accessible license. However, using the credit card in the online market can be purchased for as little as $ 450 cost. Even to hack into conversation between air controller and airplane is very easy with a small fix inside of a portable radio transmitter (Arbukle, 2009) . In the event of a real test, white hackers experts were able to create a radio capable of broadcasting signals from fake virtual aircraft. They were also able to connect a radio signal to a free online flight simulator game called Flight-Gear. Hackers used this game to create a ghost plane using ADS-B, an airplane that seemed to be real to air traffic controllers, and later astonished San Francisco International Airport systems (Henn 2012). EURECOM security researcher Andrei Costin says; in a very short time, these attacks have become laughably cheap, and of kindergarten-level technical complexity (Loo, 2013). A review by the US Government Accountability Office (GAO) in 2015 found that many points were available to jump from networked computers to National Airport (NAS) systems. The review also showed that air traffic systems were terrible in patch updates and were not great at detecting network vulnerabilities and intrusions. All this makes things really much easier for hackers (Brandom, 2017).

We found it worth to mention three of many examples of aircraft hacking incidents corroborating this argument; On October 8, 2015, Patrick, director of the European Aviation Safety

[1] Ankara Development Agency, Internal Auditing, PhD, CISA, CRISC, PMP, Ankara, Turkey
[2] Yildirim Beyazıt University, Faculty of Natural Sciences, Ankara, Turkey
*Corresponding author (İletişim yazarı) icsiacag@gmail.com

Citation (Atıf): Efe, A., Caylan, A. C., Tuzlupınar B. (2019). Siber Tehditlere Karşı Hava Trafiği Güvenliği. Bilge International Journal of Science and Technology Research, 3 (2): 135-143.

Agency, announced that he had provided critical information about the system vulnerability. The issue is that a cyber security consultant can capture aircraft by exploiting security vulnerabilities in the Aircraft Communication Addressing and Reporting System (ACARS). The ACARS system is used in the aerospace industry as a digital data link system for the exchange of short messages between airplanes and ground stations via Airband radio or satellite mechanisms. The shocking information was that the consultant only needed 5 minutes to break ACARS and a few days to access the ground-based aircraft control system.

A group of terrorists is no longer needed to take control of an airplane. Even a hacker with relatively limited tools and techniques can take control over the entire control system. Such attacks may include aircraft navigation and cockpit systems. Hackers were able to send navigation commands using radio signals to control aircraft systems using the public Flight Management System (FMS). Tools such as FMS hardware that contain some or all of the same code as systems on real planes can be purchased from eBay. Hacking seems to be very effective in two technologies: Automatic Dependent Surveillance Broadcast (ADS-B) and Aircraft Communication Addressing and Reporting System (ACARS) (Paganini, 2013, 2015).

Another white hat researcher stated that he hacked aircraft software and successfully commanded climbing while flying into engines. It is also stated that it is possible to overwrite the code in the Thrust Management Computer on the plane while flying. A white hat pirate has shown that he can successfully command the system he has accessed to command climbing. FBI agent Hurley, who conducted the investigation on this, reported: The pirate, with the codes he wrote, caused one of the aircraft engines to move to the side of the plane. Hacker used the Vortex software to monitor traffic from the cockpit system after compromising and exploiting the aircraft's networks. The hacker was said to use Kali Linux to test the penetration of the IFE system using default IDs and passwords to compromise IFE systems. The hacker used VBox, a virtualized environment to create its own version of the aircraft network ” (Kovacs, 2015).

These kind of hacking risks are stemming from insider information that is developed by practicing with ACARS as part of their professional responsibilities. But these tacit knowledge and strategic information related with vulnerabilities can always be revealed to third parties or black hat hackers. There are lots of retired pilots and engineers that have worked in the most critical air traffic systems. Even the pilots or engineers that are working in military air forces can collide with hackers or their knowledge and expertise related with critical and sensitive information of systems be exploited or traded. These kinds of risks and threats that are associated with national defense, military and air forces, missile and radar characteristics are outside of the concept boundary of our work. Here, we will work on risks and controls related with vulnerabilities of civil air traffic systems.

2. Air Traffic Control (ATC) Systems

Air Traffic Control (ATC) is to prevent aircrafts from colliding with each other or any other obstacles on the landing, departure or flight part; Air Traffic Service (ATS) type to provide fast and regular air traffic flow. The system is responsible for tracking, detecting, and descending a flight. ATM security is related with illegal access and attack. It deals with attacks that target the ATM system directly. In addition, it prevents and responds to attacks on other parts of the aviation system. The part of ATM System that matters to us is an ATM Security. It is a subset of Aviation Security which consists of Airspace Security, Airport Security and Aircraft Security. Risk assessments of Aircraft system security are required in combination with network security. Aircraft network security includes the data link, internal aircraft data bus connections, switches, and routers. The Federal Aviation Administration (FAA) faces at least three basic issues of cyber threats. These are;

- The safety of ATC System
- Safety of aircraft flight systems

Determining the distribution of tasks and responsibilities among the various FAA cyber security units.

3. Security Attributes of ATC

This paper describes essential attributes of ATC. These are used on critical and safety system. Therefore, we need to discuss security of these attributes.

3.1. Aircraft Communication Data

The communication between autopilot, flight computer, display panels, and ATC System work through a centralized, integrated communication system produces the aircraft communication data. ATC Systems perform the communication between aircraft thanks to flight computer. All necessary flight information is included in this light computer. Autopilot makes movements of the aircrafts according to flight plan. For this reason, this flight plans information is very important for security. Flight plan must not be reachable by any authorization access. In here, the risk is that if an ATC System is hacked, it starts to send incorrect information to the pilot to an extent that can cause catastrophic results (Gilbert, 2003). The aircraft are equipped with a wireless maintenance system. Attackers can access the information of the aircraft by accessing this wireless system. On this side, a maintenance-requiring aircraft can turn it into a plane threat, causing the problem to not be shown or maintained. They may have trouble on the other side of the plane without problems on the system. For this reason, such attacks can be dangerous because of the maintenance and flight cancellation on the maintenance free aircraft.

3.2. DDS Technology

The DDS is a middleware protocol and also standard of API for data-centric connectedness by the Object Management Group (OMG). It combines the system attributes which are a system together, providing low-latency data connectivity, extreme reliability, and a scalable architecture. The DDS application contains publishers and subscribers. Publishers use the data generating people to generate data, and subscriptions generate data using data readers.

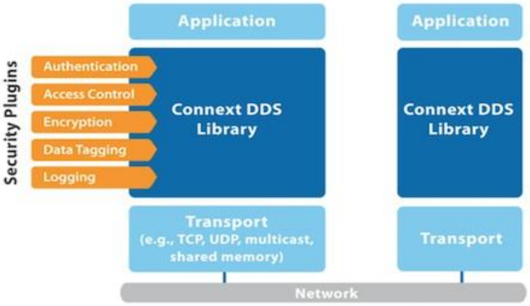


Figure 1. This figure represents layers in DDS technology (Corsaro, 2018)

For example, the reliable operation of the ATC and the Management System is depending on the lives of many people who fly over the area they manage. For this reason, these systems should ensure that critical data is delivered reliably, independently of experienced failures, by providing of 99.999 certain percentage of usability (Corsaro, 2018) . According these reasons, the system is critical which means that it does not approve any failures. Therefore, it must be taken precaution on ATC using security solutions.

3.3. Voice Information

Day by day, security needs is increasing in communication system of ATC System due to new technological abilities and knowledge advances on systems interference. Communication with the aircraft is providing by Very High Frequency (VHF) radio system. This radio system uses analogue Dual Side Band-Amplitude Modulated (DSB-AM) transmission technique which is completely open to being attacked or masked. The security threats in this area are in the mobile voice and data link communication. In the ATC System, voice change is widely used. All the pilots in a specific area must listen to the audio channel jointly. This is provided by the Medium Access Control (MAC) protocol. Not just pilots, but anyone else can listen to the voice communication channel using the same tools. This situation poses a risk of air traffic control system.

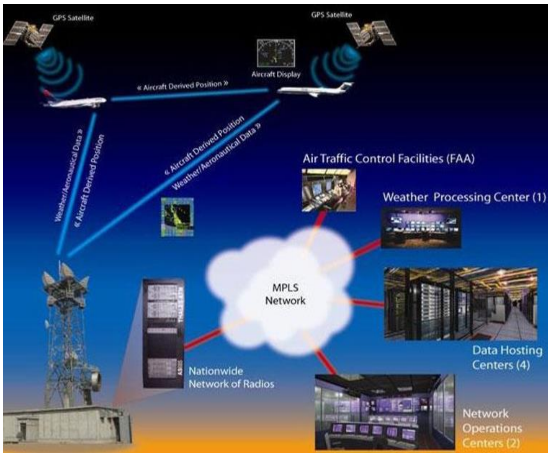

GPS Satellite
GPS Satellite
Aircraft Display
« Aircraft Derived Position »
Weather/Aeronautical Data »
« Aircraft Derived Position
« Aircraft Derived Position
Weather/Aeronautical Data »
Air Traffic Control Facilities (FAA)
Weather Processing Center (1)
MPLS Network
Data Hosting Centers (4)
Nationwide Network of Radios
Network Operations Centers (2)

Figure 2. Air Craft Voice Communication

In Fig.2, to simulate the voice communication between air craft and ground station (Gilbert *et al*., 2003). Considering other systems that an aircraft is communicating such as with weather processing center, data hosting centers nationwide networks of radios and network operations centers as is demonstrated in the Fig.3, interaction between the nodes must be secure for external attacks.

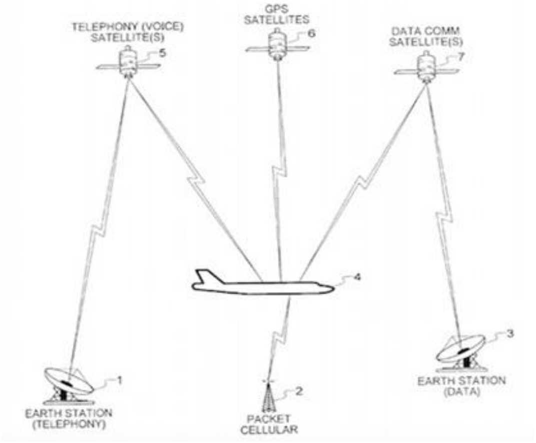


Figure 3. Depiction of Automatic Dependent Surveillance-Broadcast (ADS-B) operations (Mc.Callie, 2011)

We argue that it is related about Air Traffic Control (ATC) Centers, Communications systems, Surveillance Systems, Navigations Systems that need to be protected for security of information in air traffic system that includes operational information, such as flight plans, surveillance data, communication data (voice information, unique aircraft information, radar information etc.), and administrative information.

Goals of the ATM security as follows:

- To avoid an attack from succeeding
- To be able to respond effectively to a successful attack

4. Related Works

Academic works conducted in the area enhance our understanding of Air Traffic Management security. The content of the research follows sequence from general to specific topics. The featured topics focus of recent researches are category of information security, DDS protocol security and Air Traffic Communication Security that it is subset of cyber security literature.

John Hird and Martin Hawley describe what can be done in the SESAR project to make the ATM system safer, more flexible and more sophisticated [1]. The Single European Sky ATM Research (SESAR) is a joint project designed to completely modernize the European airspace and Air Traffic Management (ATM) with the modernization and harmonization of ATM systems through the identification, development, validation and implementation of innovative technological and operational ATM solutions.

SESAR consists of a number of different key features and concepts. One of these is System-Wide Information Management (SWIM). This defines how information shall be managed, maintained and distributed. SWIM is being developed based on a set of principles including:

- Separation of information provision and consumption
- Loose system coupling
- Use of open standards
- Use of service-oriented architecture

AIMSL is being developed in accordance with these principles. The intention is that through AIMSL, the EAD will be able to act as an Aeronautical Information Management System within the SESAR target concept and exchange information with other systems through SWIM.

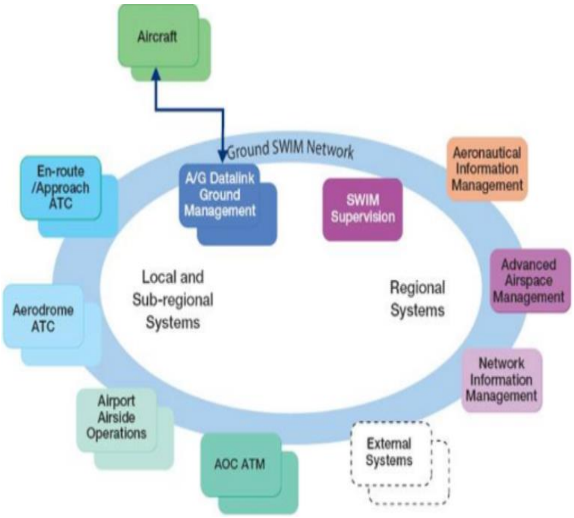

Aircraft
Ground SWIM Network
En-route /Approach ATC
A/G Datalink Ground Management
SWIM Supervision
Aeronautical Information Management
Advanced Airspace Management
Local and Sub-regional Systems
Regional Systems
Aerodrome ATC
Network Information Management
Airport Airside Operations
AOC ATM
External Systems

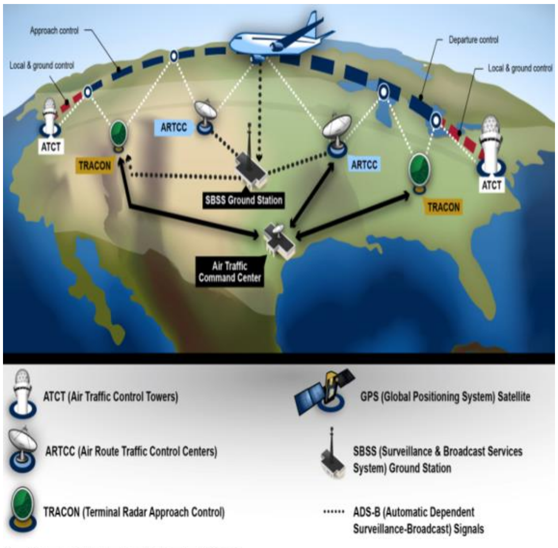
Figure 4. Communications, networks and surveillance in SESAR (Sesar, 2018)

As is demonstrated in the Fig.4, SWIM is developed in SESAR as a result of some projects which have three basic categories (SESAR, 2018):

- Information-Data Modelling
- Information-Service Modelling
- Technical Architecture of SWIM

The safety of ATMs in SESAR is examined in two ways. Self-protection/resilience: It is the resistance of the ATM system to self-protection. Collaborative support: Illegal intervention, exchange information with the necessary units such as military units from ATM. The distinction between security and safety is important. Safety concerns the undesirable causes; it causes a security event. But, security related to illegal causes that could lead to a security occurrence. The scope of security is personnel, capacity, performance, economic, branding, regulatory, environment. For example, impact of the economic can be financial loss and impact of the capacity can be reduction, loss. According to risk environment, as the dependency increases, the impact level of the attack increases. Also, using of open standard is increase likelihood of the attacks. These two terms impact and likelihood are main terms of the risk.

Skaves (2015) gives an overview about the Federal Aviation Administration aircraft systems information security protection. This paper mentions about electronic Aircraft Systems Information Security Protection. FAA can be examined in four lines of business. These are airports, air traffic organization, aviation system and commercial space transportation. In public network, increasing aircraft connectivity to aircraft systems and networks may require additional security risks. Because of the increasing risk, it should supply improved safety, security, and the environment. There are several elements in aircraft network security which are the data link, internal aircraft data bus connections, switches, and routers.


Approach control
Local & ground control
Departure control
Local & ground control
ATCT
TRACON
ARTCC
SBSS Ground Station
ARTCC
TRACON
ATCT
Air Traffic Command Center
ATCT (Air Traffic Control Towers)
GPS (Global Positioning System) Satellite
ARTCC (Air Route Traffic Control Centers)
SBSS (Surveillance & Broadcast Services System) Ground Station
TRACON (Terminal Radar Approach Control)
ADS-B (Automatic Dependent Surveillance-Broadcast) Signals

Source: GAO based on Federal Aviation Administration information. | GAO-15-221

Figure 5. Aviation Control System (Kravets, 2013)

As is demonstrated in the Fig.5, the aviation control system in the US is said to have significant weaknesses against possible cyber-attacks. United States Government Accountability Office (GAO) said in 2015 information security report: “The Federal Aviation Administration (FAA) is taking steps to protect air traffic control systems from cyber-based and other threats. Despite such measurements, some significant security control weaknesses remain. These vulnerabilities also seriously threaten the agency's ability to ensure the safe and uninterrupted operation of the national airspace system (NAS). In addition to control weaknesses or inadequacies, some shortcomings in border protection controls between less secure systems and the operational NAS environment also increase the risks associated with these weaknesses” (GAO, 2015). After comprehensive analysis and assessments over ATM of FAA, the GAO recommended 168 precautions be taken. Amongst the recommendations for improvement of security we have found those items to be the most important that need to be mentioned:

- Providing NCO with full network packet capture capability for analyzing network traffic and detecting anomalies at major network interface points at FAA operational facilities.
- Integrating network traffic flow data into NCO’s ad-hoc query systems.

- Providing NCO with access to network sensors on key network gateways for reviewing intrusion detection, network traffic, and network session data.
- Providing NCO with security event log data for all IP-connected NAS systems (GAO, 2015).

Rusko and Finke (2016) describe how to build an air traffic control system safely and how to verify that this system is safe. They used speech analysis methods to create this system. The system provides voice communication between the pilot and the air traffic controller and at the same time shows the current traffic flow. The aim of this system is to remove security vulnerabilities in the system with multimodal technique. Moreover, a system called SACom (secure air traffic control communication) is used to describe layers of security in air traffic control communications. This system has four basic particles that are independent of each other. These parts as follows:

•Speaker verification (voice communication analysis),
•Stress detection (voice communication analysis),
•Conformance monitoring (non-vocal analysis),
•Conflict detection (non-vocal analysis).

It has a disadvantage which is for threat indicator because the fact that in general, it has an important influence.

Monteiro at al, (2016) presents determining effect of cyber-attack and network system failures using open source tools in Air Traffic Control. The authors aim has several parts which are cyber and traffic control simulations, a framework depending on open source tools to combine both missions and cyber directions on ATC simulations, and a basic simulation with a fake target injection and a cyber-attack. This paper's main concept is providing semantic diagram which has five modules. These modules include such things as physical and data link emulation, network emulation, flight dynamics, surveillance protocols and pilot-controller communications. The advantage of the system is easy to simulate and test complicated infrastructure.

There some efficient schemes which are attribute-based encryption, searchable encryption, hidden vector encryption and inner product encryption. Thus, we research these schemes. In addition, one of them is most popular and has information about the others and it is most suited for cloud storage systems with huge amount of data.

Dongyoung et al, (Koo, 2013) proposed an efficient data retrieval scheme using attribute-based encryption. They embrace cryptographic background which has several attributes. These are access structure, bi-linear maps, bilinear Diffie-Hellman assumption, and anonymous key agreement scheme. They are to provide an efficient technic for rich meaningfulness as regards access control and fast searches with simple comparisons of searching entities. It is important carrying for ATC security information one station to another.

Pradhan et al. (2014) proposed an approach that the system has to make a strict information partition. This division of information is provided by the strong abstraction of communication between the publisher and the subscriber. Furthermore, DDS does not support partitioning of information based on security classifications. There are address restrictions, and there are also two contributions that provide safe access that uses a tag cage to represent security classifications. It also implements Multilevel Security (MLS) policies to perform strict information distribution. It implements an existing DDS implementation with an existing dedicated transport mechanism to perform a publish/subscribe layer with information classification based on security classifications of applications.

5. Analysis of ATC Security

For the analysis of ATC security, there should be a basis on the main concepts of security.

5.1. Security Concepts of DDS

The DDS security has several concepts which are authentication, confidentiality, integrity, non-repudiation and availability.

5.1.1. Authentication

Authentication is to verify the identities of the Authentication is to verify the identities of the principles that access the information, to limit access to information to competent authorities, using a security model in which authorization rules are expressed.

The authentication problem is being solved with certificates signed by a recognized authority. This case is essential part of security concepts. The ATC System must use certificate signs each network for preventing outside of the coverage area.

5.1.2. Confidentiality

This is to protect the information so that it can only be viewed by targeted audiences, and prevent information from being monitored or blocked. Confidentiality can be assured by hiding the content of messages from third-party observers. The preventive practices are encryption and key-exchange algorithms. These are hiding the information of flight planning, voice information, coordinating of the aircraft data (Hird, 2016).

5.1.3. Integrity

This is to prevent modification/alteration of data by a third party. The system protection must be used with integrity check and control functions or hash functions. These functions switch real data to encrypted data.

5.1.4. Non-repudiation

This is to prove it is undeniably the creator of the message. A solution is using digital signatures, system audit and log dossiers. It is guaranteed who did which operations.

5.1.5. Availability

This is to protect system and infrastructure from interruption of services and be able to use pertinent information when required. Some precautions are boundary protection and use of challenges to Limit Denial of Service Attacks which use a central machine. It checks and controls the system legitimate users. The DDS system has several advantages of distributing data. It is not enough for safety critical system. Thus, these security concepts must be added on the system in order that it is fully equipped (CSFI, 2015).

5.2. Measurements for Effective Voice Information Security

In order to protect illegal access to information systems, user accounts and access control lists (ACL) should be periodically controlled. The user must be identified and authenticated before the system is reached. Identity verification can be resolved by going to match user identity and password information.

Border protection controls are used to limit connections to and from networks, and to control connections between networked devices. Multiple security layers can be applied to protect the internal and external boundaries of an information system to decrease the risk of a successful cyber-attack. For instance, multiple firewalls can be used to prevent unauthorized access of people to systems.

The encryption method can be used to prevent the necessary information from being accessed by everyone. This method makes important information incomprehensible to unauthorized persons. Thus, system integrity is ensured and secured. Cryptographic algorithms can be applied by mathematical operations during the encryption process.

5.3. Prevention of Aircraft Communication Data

Prevention of aircraft communication data requires testing to communication and data system between airborne platform and the ground system. This testing shows that the weakness of the system. Detected weakness must be mitigated before the aircraft goes to trouble.

Data transmission in aircraft should be done by encryption and encoding in end-to-end transmission. Also, two-steps authentication mechanism can be implemented for login by thin client and ensured that not any attacks may be occurring to maintenance system. Before any of attack performed to aircraft, patch management must be planned.

5.4. Assessment and Futuristic Perspectives

We have mentioned about ATC System security in this paper. The safety critical system does not have any error on the system. Consequently, it breeds each components which have own security using valid and standard methods. That is a major and important idea on our approach and ATC System security.

In future, the system components have unique encryption and decryption. It is not enough for our approach. At the same time, they support security concepts and improvable new methods.

6. Conclusion

This paper presented our work on security of ATC Systems. It was mentioned that vulnerabilities of the ATC System are aircraft communication data, DDS protocol and voice information. Our proposed approach is improving security issues on vulnerabilities. Our inference is finding best configuration of the system which means that understanding the system properties, then using secure algorithms, techniques and methods. In our research, we collected interrelations of different elements of vulnerabilities, risks and threats on the topic. Then, we analyzed and divided to subtopics. Consequently, we selected best appropriates on the literature of ATC Security. Following recommendations can be inferred from our analysis:

1. ADS-B information which involves the two dimensional position information, the level information and the time information of the aircraft; it is possible to ensure encoding this information so that this information is invisible to the hackers.
2. The aircraft data from ADS-B may be randomly blurred within the allowed error limits for the ATC purpose. By fuzzy data, the threat cannot be completely remedied, but it can be difficult for malicious unmanned aerial vehicles (UAV) to monitor and interfere with aircraft information using ADS-B data.
3. In case of malicious unmanned aerial vehicles that provide position information control with GPS, GPS data is distorted and false position information is sent so that they can be prevented from interfering with flights.
4. Implementing robust internal network security measures on a micro-segmented infrastructure is of crucial importance for prevention.
5. Implementing real-time cyber threat detection and response capability will be very important for effective deterrence.
6. Implementing robust remote access controls will provide required safe authentication and prevention.
7. Regularly evaluating third-party and supply chain security risks will guide and help security teams with necessary consultancy.

References

Arbuckle, A. C. (2009) , https://mods-n-hacks.gadgethacks.com/how-to/hack-transistor-radio-hear-air-traffic-control-232754/ accessed February 15, 2018.

Brandom, R. (2017), https://www.theverge.com/2017/11/23/16694118/mr-robot-hack-report-s3e7-fredrick-tanya accessed February 15, 2018.

CSFI (2015), ”CSFI ATC (Air Traffic Control) Cyber security Project”,July 16, , https://scadahacker.com/library/Documents/Case_Studies/CSFI%20-%20ATC%20Cyber%20Security%20Project.pdf

Corsaro, A. (2018) ”The DDS Tutorial” http://download.prismtech.com/docs/Vortex/pdfs /OpenSplice_DDSTutorial.pdf accessed February 15,.

GAO, (2015), http://www.gao.gov/assets/670/668169.pdf accessed February 15, 2018.

Gilbert, J., Boden, S., Atkinson, R., (2003) ”Aircraft data and voice communications system and method”, February 13,.

Henn, S. (2012), https://www.npr.org/sections/alltechconsidered/2012/08/16/158758161/could-the-new-air-traffic-control-system-be-hacked accessed February 15, 2018.

Hird, J. Hawley M. and Machin, C. (2016) ”Air Traffic Management Security Research in SESAR,” 2016 11th International Conference on Availability, Reliability and Security (ARES), Salzburg, , pp. 486-492.

Kovacs, E. (2015), http://www.securityweek.com/fbi-says-researcher-admitted-hacking-airplane-mid-flight accessed February 15, 2018.

Kravets, D. , (2015), https://arstechnica.com/tech-policy/2015/03/us-air-traffic-control-computer-system-vulnerable-to-terrorist-hackers/ accessed February 15, 2018.

Koo, D. Hur, J. Yoon, H. (2013), “Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage”, Computers and Electrical Engineering, Volume 39, Issue 1, January, Pages 34-46.

Lo, C. (2013), https://www.airport-technology.com/features/featureair-traffic-control-easy-target-hackers/ accessed February 15, 2018.

McCallie, D.L. 2011, https://ecfsapi.fcc.gov /file/7021694523.pdf accessed February 15, 2018.

Monteiro, M., Sarmento, T., Barreto, A., Costa, P. and Hieb, M., (2016), ”An integrated mission and cyber simulation for Air Traffic Control,” 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, , pp. 2687-2692.

Paganini, P. (2015), http://securityaffairs.co/ wordpress/40975/hacking/easa-airplane-hacking.html accessed February 15, 2018.

Paganini, P. (2013), http://securityaffairs.co/ wordpress/13625/hacking/hijacking-planes-navigation-system-with-android-reality-or-unnecessary-alarm.html accessed February 15, 2018.

Pradhan S. et al., (2014), ”Establishing Secure Interactions across Distributed Applications in Satellite Clusters,” 2014 IEEE International Conference on Space Mission Challenges for Information Technology, Laurel MD, , pp. 67-74.

Rusko M. and Finke, M. (2016), ”Using speech analysis in voice communication: A new approach to improve air traffic management security,” 2016 7th IEEE International Conference on Cognitive Infocommunications (CogInfoCom), Wroclaw, , pp. 000181-000186.

SESAR, (2018), https://www.ead.eurocontrol.int /eadcms/eadsite/evolutions/aimsl.html, accessed February 15,

Skaves, P. (2015), ”FAA Aircraft Systems Information Security Protection overview,” 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), Herdon, VA, pp. A1-1-A1-17.