AIR PROTECTION ENCRYPTION PROTOCOLS FOR SECURING AIR TRAFFIC CONTROL COMMUNICATION

Valentin PREDA[*], Răzvan GHICA[*], Iulian BLENDEA[*], Dumitru DIACU[*], Alin GHIȚĂ[*], Andrei-Mihai LUCHIAN[**]

[*]National Polytechnic University of Science and Technology Bucharest, Romania (preda.valix@gmail.com, alexandru.ghica@stsnet.ro, iulian.blendea@stsnet.ro, diacudorin@yahoo.com)
[**]Special Telecommunications Service, Bucharest, Romania (alin.ghita@stsnet.ro, riesigen@gmail.com)

DOI: 10.19062/1842-9238.2024.22.1.2

Abstract: *The article presents a detailed analysis of the encryption protocols used in air traffic control systems to ensure the security of communication between aircraft and ground systems. The importance of secure communication in air traffic management is highlighted and encryption protocols such as AES, RSA and ECC are examined within the specific context of air traffic control. Special emphasis is placed on secure communication architecture and cryptographic key management solutions. Challenges and solutions in implementing these protocols in complex environments with high security requirements are also discussed.*

Keywords*: encryption, security, air traffic control, encryption protocols, AES, RSA, ECC, secure architecture, cryptographic key management, air communications.*

1. INTRODUCTION

Air traffic control systems (ATC - Air Traffic Control) represent an essential infrastructure in the safe and efficient management of air traffic globally. These systems are responsible for monitoring and guiding aircraft in the airspace, ensuring that flights are carried out safely and according to established rules.

The importance of secure communication within air traffic control systems cannot be understated. Accurate and rapid communication between air traffic controllers and pilots is critical to collision prevention and emergency management. In such a dynamic and complex environment, every piece of information transmitted must be protected against interception or modification by unauthorized parties. [1]

The introduction of encryption protocols is a critical component in ensuring the security of air communication. Encryption is the process of transforming data into a format unreadable by those who do not have the appropriate decryption key. Thus, even if messages are intercepted, they remain incomprehensible to attackers. [2]

The statement of the problem comes in the context of the identification of vulnerabilities in air traffic control systems. With increasing interconnectivity and dependence on technology, these systems are becoming increasingly exposed to various cyber threats. Attacks on infrastructure ATCs can have serious consequences, including disrupting air traffic and even endangering the lives of passengers and flight crews. [3]

In this regard, it is imperative to implement robust encryption measures to protect communication and data within air traffic control systems. Strong encryption provides an effective barrier against the interception and manipulation of sensitive information, helping to strengthen aviation security.

2. PRESENTATION OF AIR TRAFFIC CONTROL SYSTEMS

The role of air traffic control is crucial in ensuring safe, efficient and orderly air travel. These systems and procedures are designed to manage the movement of aircraft in airspace, prevent collisions and facilitate the flow of traffic in an organized manner. Through air traffic control, coordination is ensured between aircraft and controllers to maintain safe distance and guide aircraft to their destinations in an efficient manner. [4]

The main components of air traffic control systems include:

Ground-Based Radar: Radar is an essential tool for monitoring and detecting aircraft in airspace. Ground-based radar uses radio emissions to detect and track moving aircraft. This information is transmitted to air traffic control centers, where controllers use this data to guide flights safely.

Communication systems: Communication between controllers and pilots is essential for flight coordination. Communication systems enable the rapid and accurate exchange of information between controllers and flight crews. These systems include dedicated radio frequencies as well as voice and data communication channels. [5]

Aircraft Avionics: Avionics is the set of electronic systems and instruments installed on aircraft for navigation, communication and control. These systems include equipment such as transponders, which transmit information about the identity and position of the aircraft to air traffic controllers, and advanced navigation systems, which help pilots follow planned routes and avoid obstacles during flight. [6]

The functionalities of air traffic control systems include monitoring air traffic, guiding aircraft on safe and efficient trajectories, managing airspace to avoid collisions, and facilitating communication between controllers and pilots. Through these advanced systems and technologies, it is ensured that flights are carried out safely and according to air traffic rules.

3. ENCRYPTION PROTOCOLS FOR AIR TRAFFIC CONTROL SYSTEMS

In air traffic control systems, various encryption protocols are used to ensure the confidentiality and integrity of communications between aircraft and ground systems. These include:

1. AES (Advanced Encryption Standard): AES is one of the most widely used symmetric encryption algorithms today. It is efficient and offers high security. AES is primarily used to encrypt data transmitted between aircraft and air traffic control centers to protect sensitive information.

2. RSA (Rivest–Shamir–Adleman): RSA is an asymmetric encryption algorithm that uses a pair of public and private keys. It is often used for key exchange and authentication in secure communications. In air traffic control, RSA can be used to ensure the confidentiality and authenticity of messages transmitted between aircraft and control centers.

3. ECC (Elliptic Curve Cryptography): ECC is another asymmetric encryption algorithm known for its resource efficiency and the high level of security it provides. In air traffic control systems, ECC can be used to encrypt and authenticate data transmitted between various infrastructure components.

How encryption ensures the confidentiality and integrity of communication:

Encryption is essential to ensure the confidentiality and integrity of communication in air traffic control systems. Through encryption, data transmitted between aircraft and ground systems is transformed into a format unreadable by anyone who does not possess

the appropriate decryption key. Thus, even if the data is intercepted by an attacker, it remains incomprehensible and unusable. [7], [8]

Encryption also ensures data integrity, as any attempt to change the encrypted information can be detected by the recipient who decrypts the message. Additionally, encryption algorithms can be combined with hash functions to verify data integrity.

Criteria for selecting encryption protocols in air traffic control:

In choosing encryption protocols for air traffic control systems, several factors are considered, including:

• Computational efficiency: Encryption protocols should provide a high level of security without compromising systems performance.

• Resistance to cryptographic attacks: Protocols must be resistant to attacks such as cryptanalysis and brute force.

• Compatibility and interoperability: The selected protocols should be compatible with the existing infrastructure and allow efficient communication between the different components of the air traffic control system.

• Updates and standards: It is important that encryption protocols comply with current security standards and are regularly updated to address new threats and vulnerabilities.

Through careful evaluation and selection of encryption protocols, it is ensured that communication in air traffic control systems remains secure and protected against cyber threats. [9]

4. ENCRYPTION PROTOCOLS FOR AIR TRAFFIC CONTROL SYSTEMS

This chapter proposes a secure communication architecture specifically adapted for Air Traffic Management (ATM) systems. The main purpose of this architecture is to provide a robust framework for ensuring the confidentiality, integrity and authenticity of data in communication between aircraft, air traffic control centers and other entities involved in air traffic management.

Layered approach to security:

The proposed architecture is based on a layered approach to security, which integrates multiple levels of protection to ensure a secure communication environment. This includes:

1. Encryption: Use of encryption algorithms such as AES, RSA or ECC to protect data transmitted between the various components of the ATM system. Encryption ensures the confidentiality of information by converting it into a format that is unreadable by anyone who does not have the appropriate decryption key.

2. Digital signatures: Implementation of digital signatures to ensure the integrity of transmitted data and to confirm the authenticity of messages. By using digital signatures, it is guaranteed that the data has not been altered in transit and that it comes from the declared source.

3. Authentication mechanisms: Integrating authentication mechanisms, such as digital certificates or multi-factor authentication protocols, to verify the identity and access rights of communication participants. These mechanisms ensure that only authorized entities can access and communicate within the ATM system. [10]

Effective key management practices: A crucial aspect of the architecture is the management of the cryptographic keys used to encrypt and decrypt data. To ensure system security and reliability, effective key management practices are implemented, including:

• Secure Key Generation: Using secure cryptographic algorithms to generate cryptographic keys so that they are resistant to brute force and cryptanalytic attacks.

• Secure Key Distribution: Implementing secure protocols for key distribution to authorized participants within the ATM system, ensuring that keys are transmitted in a confidential and authentic manner.

• Secure key storage: Using secure key storage mechanisms, such as hardware security modules or key management systems, to prevent unauthorized access to cryptographic keys. [11], [12]

By implementing a secure communication architecture based on these principles and practices, air traffic management systems can ensure a secure communication environment protected against cyber threats and information security risks.

5. SECURE COMMUNICATION ARCHITECTURE FOR AIR TRAFFIC MANAGEMENT SYSTEMS

Proposal of a Secure Communication Architecture Adapted for Air Traffic Management Systems:

The proposed architecture for Air Traffic Management (ATM) systems is built upon robust cybersecurity principles, with the primary objective of ensuring the confidentiality, integrity, and authenticity of communications within these critical systems. The architecture is designed to efficiently manage communication among various entities involved in air traffic control, including air traffic controllers, aircraft, and other components of the ATM infrastructure.

Layered Security Approach:

The architecture is based on a layered security approach, integrating multiple levels of protection to ensure a secure communication environment. This approach includes:

Encryption: Utilizing strong encryption algorithms such as AES, RSA, or ECC to encrypt data transmitted between various components of the ATM system. Encryption ensures data confidentiality, protecting them against interception and unauthorized access.

Digital Signatures: Implementing digital signatures to guarantee data integrity and message authenticity. Digital signatures are used to verify that the data has not been altered in transit and that it originates from the declared source.

Authentication Mechanisms: Integrating robust authentication mechanisms, such as digital certificates or multi-factor authentication protocols, to verify the identity and access rights of communication participants. These mechanisms ensure that only authorized entities can access

Efficient Key Management Practices:

• A crucial aspect of the architecture is the efficient management of cryptographic keys used for data encryption and decryption. To ensure the security and reliability of the system, efficient key management practices are implemented, including:

• Secure Key Generation: Using secure cryptographic algorithms for generating cryptographic keys, ensuring they are resistant to brute-force and cryptanalytic attacks.

• Secure Key Distribution: Implementing secure protocols for distributing keys to authorized participants within the ATM system, ensuring that keys are transmitted in a confidential and authentic manner.

• Secure Key Storage: Utilizing mechanisms for secure key storage, such as hardware security modules or key management systems, to prevent unauthorized access to cryptographic keys.

• By implementing this secure communication architecture, air traffic management systems can ensure a secure and protected communication environment against cyber threats and information security risks.

6. COMMUNICATION SECURITY IN DRONE OPERATIONS

Communication in drone operations is a crucial aspect for the functioning and control of these unmanned aerial vehicles. Beyond the benefits offered by drones in various fields, including military, surveillance, or civilian applications such as deliveries or imaging capture, ensuring communication security is essential for preventing unauthorized access, interception, or manipulation of transmitted data, and for avoiding potential incidents.

Vulnerabilities in Drone Communications

1. Unauthorized interception: Due to the wireless nature of communications, there is a risk that an attacker could intercept and eavesdrop on communications between the drone and its control station or between the drone and other connected devices. This interception could lead to the exposure of sensitive information or compromise of operations.

2. Jamming attacks: Jamming attacks involve disrupting or blocking the communication signal between the drone and its controller. These attacks can be carried out using specialized devices that emit strong radio signals, resulting in loss of control over the drone and potential incidents.

3. Data manipulation: Another risk is the possibility of an attacker manipulating the data transmitted between the drone and its controller. Through "man-in-the-middle" attacks, an attacker can modify or falsify transmitted data, misleading the drone operator and compromising operations.

Security Measures for Drone Communications

1. Encryption of Communications: Using strong encryption protocols to protect the data transmitted between the drone and its controller. Encryption ensures the confidentiality of information and protects against interception and unauthorized access.

2. Authentication and Authorization: Implementing robust authentication and authorization mechanisms to verify the identity and access rights of the parties involved in drone communications. These mechanisms help prevent unauthorized access and data manipulation.

3. Frequency and Channel Diversification: Utilizing technologies that allow for the diversification of frequencies and communication channels to reduce the risk of interference and jamming attacks.

4. Continuous Monitoring and Anomaly Detection: Implementing continuous monitoring and anomaly detection systems to quickly identify and counteract any attempted attacks or suspicious behavior in drone communications.

By adopting these security measures and implementing appropriate protocols and technologies, a high level of security can be ensured in drone communications, contributing to the protection of information and the prevention of potential incidents or cyber attacks.

7. CASE STUDIES OR EXAMPLES

Successful implementations of encryption protocols in securing communications within drone operations are essential for protecting sensitive data and operational information transmitted between operators and drones. Encryption is used to ensure confidentiality, integrity, and authentication of data during drone operations, helping to mitigate security risks and improve the resilience of aerial communication networks.

An illustrative example of the successful implementation of encryption protocols in drone operations is their use in military, security, and surveillance applications. In these

scenarios, drones are often used for collecting and transmitting sensitive data, such as images and videos from strategic locations or events of interest.

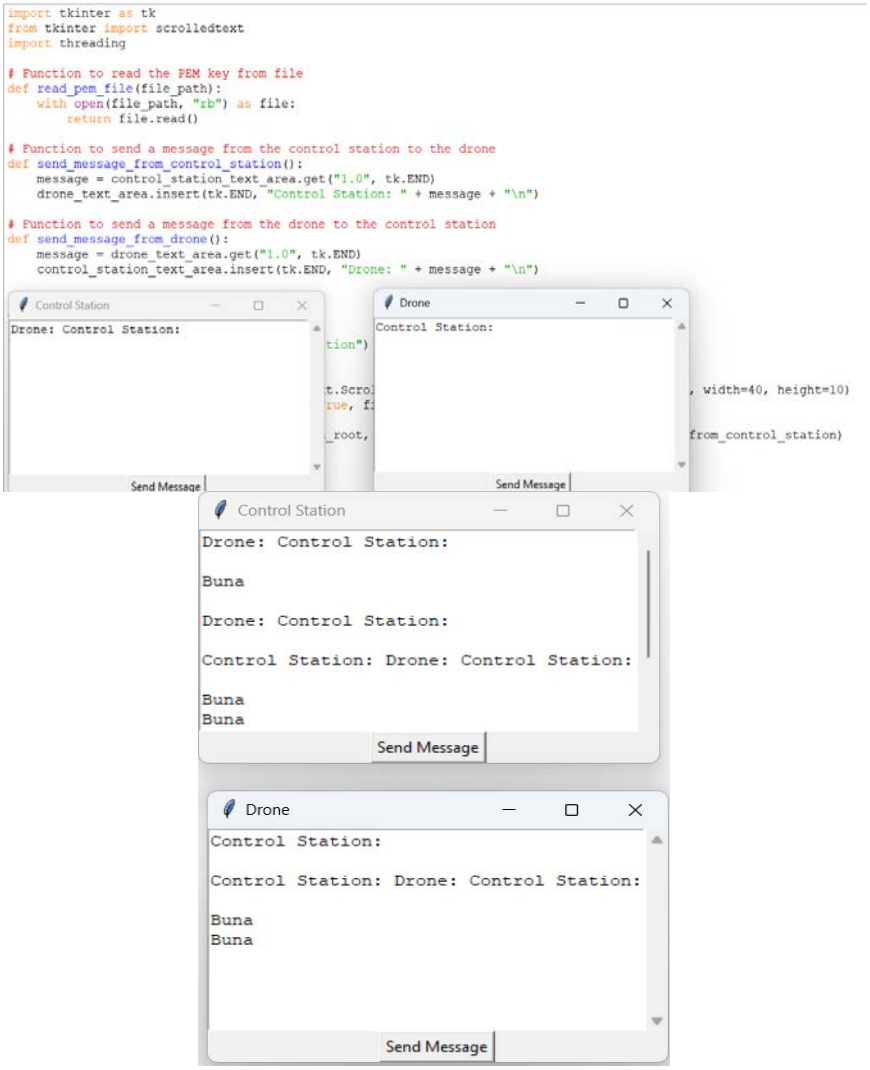
The effectiveness of encryption in reducing security risks and improving the resilience of aerial communication networks in drone operations can be highlighted through:

1. Confidentiality: Encrypting data transmitted between operators and drones ensures that sensitive information, such as images and videos from sensitive locations, cannot be intercepted or accessed by unauthorized third parties.

2. Encryption protocols enable mutual authentication between operators and drones, confirming the identity of each party involved in communication and preventing any attempt at impersonation or unauthorized access to drone systems.

3. Resilience to Cyber Attacks: Encrypting data during drone operations helps protect against potential cyber threats, such as communication interception, ransomware attacks, or other attacks on the integrity and security of systems.

- **Python Application for Encrypted Communication between Control Station and Drone Using PEM.**



In conclusion, implementing encryption protocols in securing communications within drone operations is essential Authentication for ensuring the protection of sensitive data and information, contributing to the reduction of security risks and the improvement of the resilience of aerial communication networks.

Python Code for Generating PEM Using an RSA Private Key

```
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.backends import default_backend
# Generăm o cheie privată RSA
private_key=rsa.generate_private_key(public_exponent=65537,key_size=2048,
backend=default_backend())
# Salvăm cheia privată în format PEM
pem = private_key.private_bytes(encoding=serialization.Encoding.PEM,format=
serialization.PrivateFormat.PKCS8,encryption_algorithm=serialization.NoEncryption())
# Scriem cheia privată într-un fișier PEM
with open("control_station_private_key.pem", "wb") as pem_out:
    pem_out.write(pem)
print("Cheia privată a stației de control a fost generată și salvată în fișierul
'control_station_private_key.pem'")
```

Python Code for Reading PEM

```
<cryptography.hazmat.bindings._rust.openssl.rsa.RSAPrivateKey object at 0x000002
9D3F511E50>
from cryptography.hazmat.primitives import serialization
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.backends import default_backend
# Se deschide fișierul cheii private în modul citire binară
with open("C:/Users/Andrei/Desktop/Articole Revista nr. 2, revista academiei
2023/control_station_private_key.pem", "rb") as key_file:
 # Se încarcă cheia privată  control_station_private_key =
erialization.load_pem_private_key(
 key_file.read(),
 password=None,  # Dacă cheia este protejată cu o parolă, introduceți parola aici
 backend=default_backend()  )
# Afișăm cheia privată încărcată
print(control_station_private_key)
```

8. CONCLUSIONS

In conclusion, the implementation of encryption protocols in securing communications within drone operations is an essential necessity for ensuring the integrity, confidentiality, and authenticity of information transmitted between drones and control stations. Through the analysis and development of appropriate cryptographic solutions, the following aspects have been highlighted:

1. Protection of Sensitive Data: Efficient encryption of aerial communications with drones provides robust protection against interception and unauthorized access to transmitted data, including flight coordinates, captured images and videos, as well as other relevant operational information.

2. Reduction of Security Risks: Implementing encryption protocols significantly contributes to reducing security risks associated with cyber threats, ensuring that transmitted data is protected against attacks and unauthorized access.

3. Improvement of Resilience of Aerial Communication Networks: Encrypting communications between drones and control stations enhances the resilience of aerial communication networks, increasing their capacity to withstand cyber attacks and other security threats.

4. Standardization and Proper Implementation: It is essential to adopt security standards and properly implement encryption protocols within drone operations, ensuring compliance with the highest standards of security and data protection.

5. Continued Development of Cryptographic Technology: As cyber threats evolve constantly, it is crucial to continue the development and innovation of cryptographic technology to address future challenges and ensure the security of drone communications against increasingly sophisticated adversaries.

In conclusion, by implementing encryption protocols and adopting robust security practices, the drone operations industry can advance towards increased security and more effective protection of sensitive data, contributing to strengthening trust in the use of these technologies in a growing range of applications.

REFERENCES

[1] A. Evans, D. Hodgson, A. J. Ruppert, *Introduction to Air Transport Economics: From Theory to Applications*, Routledge, 2013;
[2] W. L. Mueller, B. N. Agrawal, *Airport Operations*, CRC Press, 2018;
[3] P. Rozenberg, *Air Traffic Control: Human Performance Factor*, CRC Press, 2011;
[4] P.J. Smith, *Air Traffic Management: Economics Regulation and Governance*, Routledge, 2011;
[5] R. L. Helmreich, E. Salas, D. Maurino, J. R. Huddlestone, *Crew Resource Management*, Academic Press, 2017;
[6] A. Gardi, I. Marchetti, *Air Traffic Control: An International History*, Routledge, 2016;
[7] D. Salomon, *Data Privacy and Security: Encryption and Information Hiding*, Springer, 2017;
[8] M. J. Bach, *The Design of the UNIX Operating System*, Pearson Education, 2014;
[9] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson, 2017;
[10] M. Soriano, R. Trapero, J. Luna, J. Villalba, D. Díaz-Sanchez, S*ecure Communication Architectures for Air Traffic Management*, IEEE Aerospace and Electronic Systems Magazine, 2017;
[11] L. Girão-Silva, P. Jesus, P. Simões, M. Silva, P. Sousa, *Enhancing Air Traffic Management Communications Using a Secure MPLS-Based Architecture*, IEEE Transactions on Intelligent Transportation Systems, 2014;
[12] S. D'Antonio, L. P. Cordella, G. Desolda, C. Gravino, *Security in Air Traffic Management: A Case Study on the Development of a Secure Communication Architecture*, IEEE Access, 2019.