Security Enhancements of the Surveillance Data Exchange Protocol “ASTERIX”

Marián JANČÍK¹,*, Johannes DE HAAN² and Petr JONÁŠ³

¹,²Eurocontrol, Rue de la Fusée 96,1130 Brussels, Belgium
³Department of Air Transport, Faculty of Transportation Sciences, Czech Technical University in Prague

*Corresponding author

Keywords: Asterix protocol, Cyber Security, Radar, Surveillance.

Abstract. The surveillance information are key data for all air navigation service providers which are responsible for the safety of the air passengers and the efficiency of Air Traffic Management system. In this paper, we have focused on the analysis of a protocol used to carry the surveillance information from the sensor to the ATC centre as well as amongst variety of ATM applications inside the ATC centre. As the original ASTERIX protocol has been developed without any security mechanism, it constitutes a major vulnerability. This deficiency has been acknowledged by the AMG (ASTERIX management group) which is seeking a remedy. In this article we describe a proposal to implement the security features into the protocol.

Introduction

ASTERIX (short for “All Purpose Structured Eurocontrol Surveillance Information Exchange”) is a de-facto standard protocol defining the low level (“down to the bit”) implementation of a data format for exchanging surveillance-related information amongst ATM (Air Traffic Management) applications.[1]

It was designed as Presentation and Application protocol (layers 5 and 6 of ISO/OSI Reference Model) for communication media with limited bandwidth. This is why it follows rules that enable it to transmit all the information needed, with the smallest data load possible.

The first version of ASTERIX was approved by Radar Systems Specialist Panel (RSSP) at their 15th Meeting held on 1-4 July 1986. Nowadays it has been adopted by the world users’ community as the de-facto standard in this domain.[2] EUROCONTROL (European Organisation for the Safety of Air Navigation) is also developing a reference ASTERIX library called E-ARCO (EUROCONTROL’s Asterix Codec), which will be made available to the community free of charge.

ASTERIX is an extensible format with a number of different data categories, each of which deals with one particular kind of information.[3] These include target reports from surveillance sensors such as radars as well as processed information such as aircraft tracks and various system status messages.[4]

The structure of ASTERIX data block, which is basically the payload of the underlying TCP/IP protocol, can be defined as shown on Fig. 1:

**Figure 1. ASTERIX Data Block.**

Up to 256 Data Categories can be defined and they are available for applications in the areas listed in Table 1:[1].
### Table 1. ASTERIX Data Categories.

| Data Categories | Application                                 |
|-----------------|---------------------------------------------|
| 000 – 127       | Standard Civil and Military Applications    |
| 128 – 240       | Special Civil and Military Applications     |
| 241 – 255       | Civil and Military Non-Standard Application |

ASTERIX protocol is very efficient but absolutely lacks any safety or security (e.g. encryption) mechanisms.

### Current Status

The protocol itself is not implicitly secure. In fact there already exists a proof of concept work to exploit it. A custom software program called “MITMAST” (Man in the middle ASTERIX) which is using ARP Poisoning technique between two hosts is capable of manipulating the ASTERIX data.[5]

Despite the lack of any security feature, every air navigation service provider, the main consumer of the surveillance data, must ensure the data transported by the ASTRIX protocol are delivered securely from the sensor to the ATM centre.[6]

Besides that the ATM cyber-security in the European Union (EU) is also mandated by EU law, i.e.:
- “Commission Implementing Regulation (EU) 2017/373 - of 1 March 2017 - laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight”,
- “Directive 2016/1148/EU of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”.

To overcome the vulnerability of the protocol, the data between the sensors and the input/output gateway to the ATC centre should flow through an encrypted VPN (Virtual Private Network) or secured tunnels.[7] The Fig. 2 shows the example of a typical layoff of such arrangement.

![Air Traffic Center - Secure environment](image)

Figure 2. ATC centre example.

It shall be noted that inside the ATC centre the data are usually transported on virtual LAN or separate network segment, but they are not encrypted. Therefore the malicious acts (deliberate or accidental) from inside the ATC centre could significantly affect provided air navigation services.
Additionally, the security at the network level is continuously being scrutinised by the hackers and cybercriminals. The SSL/TLS protocol suffered during the last years several serious vulnerabilities, therefore, to put the security just in this protocol it is not enough.

Requirements

Usually, there are six main security services provided by secure communication systems: Confidentiality, Authentication, Integrity, Non-repudiation, Availability and Authorization.[8] However, for the implementation of the security elements into the ASTERIX protocol only the following main requirements have been selected.

- Authentication
- Integrity
- Confidentiality

Authentication

It must be possible to ensure that the data are coming from the expected source, e.g. a sensor. We also must ensure that the request for the data is coming from a legitimate user e.g. STCA (Short Term Conflict Alert) application.

A possible solution is to sign the data.

Integrity

The protocol shall ensure that no-one can tamper with the date once they are sent. The solution which are being considered are encryption or hashing.

Confidentiality

The protocol shall also ensure the delivery of the data over non-secure connections.

This can be achieved by encryption of the sensitive data.

Non-repudiation is considered as unnecessary in the exchange of surveillance data, due to the extremely short validity of the data. For example, the classical radar delivers the position of the aircraft every 4-12 seconds, and the modern non rotating sensors deliver the data at even higher frequency.[9] Even if the report is missed, in couple of seconds a new one will arrive.

Availability is difficult to achieve at the protocol level and besides the all ATM systems are designed and manufactured as redundant at multiple levels.

Authorization is at this time not essential. The current design of the ATM system is such that the surveillance information are provided almost directly from the producer (e.g. radar) to the consumer (e.g. SDPS - surveillance data processing systems). This allows relatively easy way to permit/deny the access to data (e.g. from the military radar).

Additional requirements which has to be considered are backward compatibility with current version of ASTERIX and compatibility with the SWIM (System Wide Information Management) systems.

Solutions

Two solutions were under consideration [10]. In both cases the ASTERIX Payload (see Fig.3 and Fig. 4) would be the whole ASTERIX data block as defined in [1] and it may or may not be encrypted, depending on the user needs. Providing that the data in the payload are not encrypted, stripping down the headers and keeping only the payload would ensure the backward compatibility with existing systems with a minimal effort.
Non ASTERIX Wrapper

The idea of having a wrapper around of ASTERIX data block would probably allow a quicker implementation, however with a significant risk that different manufacturers would implement incompatible wrappers.

Special ASTERIX Category

Similar to the wrapper this solution would also encapsulate the ASTERIX data block. The difference is that it would be standardised by AMG which would minimise the risk of incompatibility.

ASTERIX Category 000 is a primary candidate to be this special category.

PKI (public key infrastructure) is suggested for the signing, emitting and maintaining certificates and revocations lists. EUROCONTROL will in the near future start to operate the Root Certification Authority for all SWIM systems and applications. Thus using PKI is a preferred choice, however other solutions e.g. symmetric key encryption might be used as well.

Conclusion

The surveillance sensors and the surveillance network are fundamental for the safety of air transportation and consequently they are part of the critical infrastructure of every country.[11] Therefore we must make every effort to guarantee the maximum availability and security. ASTERIX protocol is very efficient but lacks any safety or security mechanisms. That is why the users have to move to another link layer to obtain a security level, which might be insufficient, considering the criticality of the carried information.

EUROCONTROL, as the lead designer of the protocol, must address the growing concerns about the security flaws.[12]

In this paper we cover the current status and we identify the main security requirements.

Our proposed mitigation against the vulnerability is to implement a special ASTERIX category which would encapsulate the transported ASTERIX categories, comparable to encapsulation principal of the data through different layer of TCP/IP protocol.

Last but not least, we highlight the need for the backward compatibility to ensure seamless cooperation with the existing systems.

References

[1] EUROCONTROL Specification for Surveillance Data Exchange - Part 1, Edition: 2.4, Brussels 2016, Reference nr: EUROCONTROL-SPEC-0149, ISBN: 978-2-87497-028-3.

[2] Dzunda, M., Hrban, A.: Accuracy of the passive tracking systems. Conference: 12th International Conference on Microwaves and Radar (MIKON98) Location: Krakow, Poland Date: May 20-22, 1998, Pages: 216-220.

[3] Novak, A., Skultéty, F., Kandera, B., & Lusiak, T. (2018). Measuring and testing area navigation procedures with GNSS. Paper presented at the MATEC Web of Conferences volume 236, https://doi.org/10.1051/matecconf/201823601004.
[4] Dzunda, Milan; Kotianova, Natalia; Pulis, Pavel; et al.: Selected Aspects of the Windmill Construction Impact on Air Traffic Safety. Conference: International Conference on Power, Energy Engineering and Management (PEEM) Location: Bangkok, Thailand, Date: January 24-25, 2016, Pages: 290-294.

[5] Casanovas, Eduardo & Exequiel Buchaillot, Tomas & Baigorria, Facundo. (2016). Vulnerability of Radar Protocol and Proposed Mitigation. Journal of ICT Standardization. 4. 65-86. 10.13052/jicts2245-800X.414.

[6] Dzunda, M.; Csefalvay, Z.; Kotianova, N.: Target Localization by Method of Intersections of the Ellipses Using Two UWB Radar Systems. Conference: International Conference on Advanced Educational Technology and Information Engineering (AETIE) Location: Beijing, Peoples R China Date: May 17-18, 2015, Pages: 697-706.

[7] Jancik, Marian, Simon Holoda, Milan Dzunda, and Branislav Kandera. “Current Status of Cyber Security in the Surveillance Data Processing Systems in Europe.” In 2018 XIII International Scientific Conference - New Trends in Aviation Development (NTAD), 59–63. Kosice: IEEE, 2018. https://doi.org/10.1109/NTAD.2018.8551678 , Electronic ISBN: 978-1-5386-7918-0.

[8] Dzunda, Milan; Kotianova, Natalia: Selected Aspects of Applying Communication Technology to Air Transportation. International Conference on Computer Science and Information Engineering (CSIE) Location: Bangkok, Thailand, Date: June 28-29, 2015, Pages: 1-7.

[9] Dzunda, M., Kotianova, N., Holota, K., et al.: Use of Passive Surveillance Systems in Aviation. Activities in Navigation: Marine Navigation and Safety of Sea Transportation, Published: 2015, Pages: 249-253.

[10] Johannes DE Haan, Eurocontrol Internal Document, “ASTERIX Security Implementation Options”, Date: NOV-22-2018, Brussels.

[11] Dzunda, M.; Cekanova, D.; Cobirka, L.; et al.: Protection Against High-Frequency Radiation of Aviation Electronic Support Systems Used in Air Transport. Transnav-International Journal on Marine Navigation And Safety Of Sea Transportation Volume: 12, Issue: 1, March 2018, Pages: 183-186.

[12] Holoda, S.; Zacik, N.; et. al. 2018. Multi-static primary surveillance radar data simulation, In Proceedings of the 4th International Conference on Traffic and Transport Engineering (ICTTE), 1-6, ISBN 978-86-916153-4-5.