Volume XXI, 41 – No. 2, 2019, DOI: 10.35116/aa.2019.0012

CURRENT STATUS OF CYBER SECURITY IN ARTAS SURVEEILLANCE DATA PROCESSING SYSTEM

Marián JANČÍK
EUROCONTROL, Rue de la Fusée 96, 1130 Brussels
Peter DZUROVČIN
Technical university of Kosice, Faculty of Aeronautics, Rampova 7, 041 21 Košice
**Corresponding author.* E-mail: marian.jancik@eurocontrol.int

Abstract. The objective of this paper is to present a comprehensive status of cyber security challenges in ARTAS surveillance data processing system. The cyber security is a major concern of current Air Traffic Systems. It is mandated by European Union as well as national law. Therefore, EUROCONTROL as the provider the ARTAS application conducted a comprehensive security assessment is to identify security vulnerabilities of the systems. For this purpose, a grey-box penetration testing was conducted by EUROCONTROL's security experts. The numerous findings are currently mitigated by the fact that ARTAS systems should be isolated and restricted in a secure architecture. The next version of ARTAS application is addressing the most critical issues.

Keywords: Cyber security; surveillance; ARTAS; tracker; ASTERIX

1. INTRODUCTION

Increasing reliance on inter-connected ATM (Air Traffic Management) systems, services and technologies increases the risk of cyber-attacks. Such risks undermine the vision of a safe, resilient and trustworthy European aviation sector, and would incur costs on the response to and recovery from cyber-attacks [1, 10, 11].

Cyber-security is mandated by the European Union law i.e.

- "Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010 concerning measures for a high common level of security of network and information systems across the Union"
- "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"

Therefore, Air Navigation Service Providers and the industry must address these growing concerns about the risks from increased automation, connectivity and reliance on digital information and systems.

One of those system is "Tracker" which process the data from the sensors (e.g. radar, ADS-B, WAM, etc.) and maintains a real-time air situation. In Europe, the most widely used tracker called ARTAS ("Atm suRveillance Tracker and Server") tracks close to 90% of European daily flights at 43 air traffic control canters [2].

2. EVOLUTION OF CYBER SECURITY PERCEPTION IN ATM

As many of the components of the current surveillance chains, including ARTAS, were developed in the late 1980s, early 1990s and the sensors even earlier, these systems were developed without any cyber-security requirements [3][4].

The security was achieved by other means:
- the networks used by the systems are physically isolated from the internet.
- the system is physically located within a secure and restricted building, where only authorised personnel have access.
- the system is operated by trained/certified operators.

Above means of security threats mitigation remains still valid up to the certain level, however especially the second threat mitigation method is less and less feasible as nowadays the networks are interconnected though usually isolated e.g. by using VPN (Virtual Private Network).

Additionally, the standardisation and usage of COTS (Commercial off the Shelf) products increased the number people who understand the technology or the protocols and are therefore capable to perform malicious attack.

As shown on Figure 1 the Air Traffic Centre is considered as secure environment and the cyber security barriers are placed at the outer perimeter.

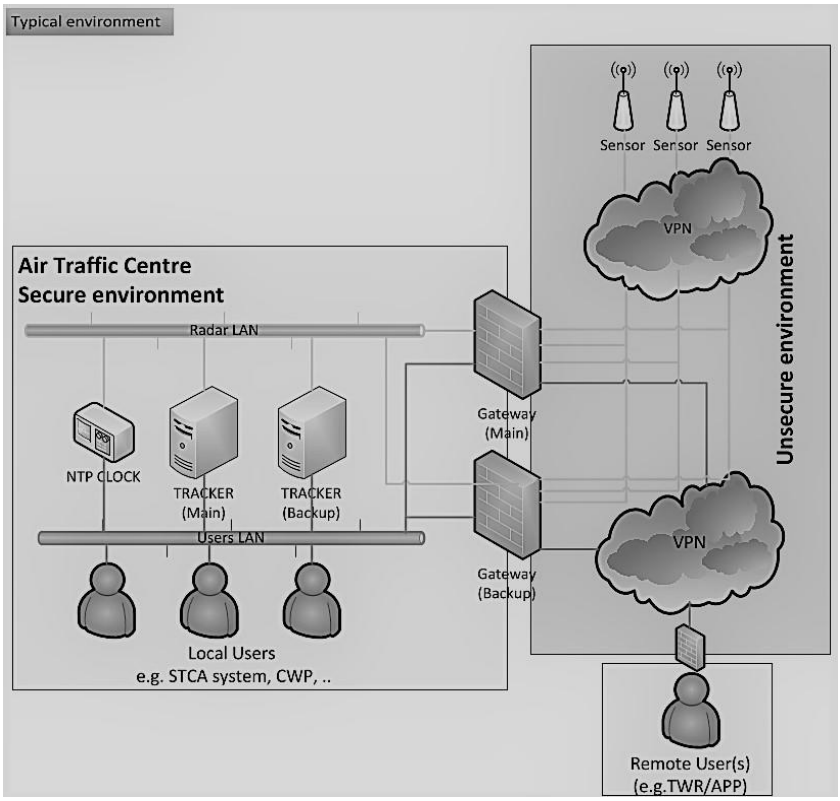

Figure 1 Example of ATC environment

2. SECURITY ASSESMENT OF ARTAS

ARTAS development started in early 1990 and security requirement were not considered. In fact, the Operating System was deliberately configured to remove security defences in order to improve the operator's freedom i.e. ease of access and to reduce the reaction time to investigate tracking related problems.

The system has undergone the security assessment, which was performed by the EATM-CERT in October 2017. Three different paths were followed during the assessment, the first two ("Compromise operating System" and "Compromise ARTAS application") constitute attack scenarios for ARTAS whereas the third path ("Attack ASTERIX") does not concern ARTAS itself but rather ASTERIX as a protocol.

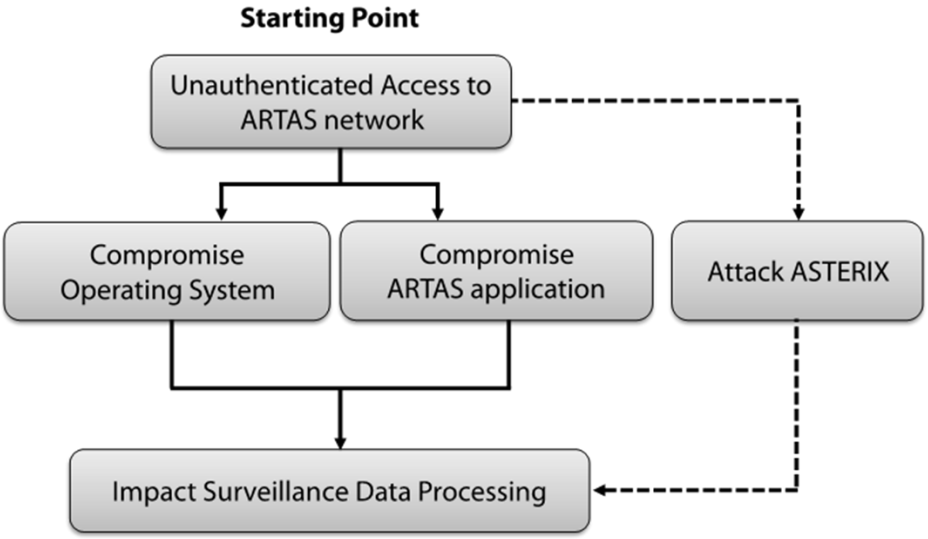

Figure 2 Attacking path

2.1. Attack on Operating System

Regarding the leftmost path of the assessment (see Figure 2), it was possible to compromise the Operating System of ARTAS by exploiting multiple vulnerabilities. See Figure 3. However, these vulnerabilities were already known and were kept on purpose, as they contribute to improve the operator's ease of use (e.g. using same password as the username). Other measures in place (isolation from Internet, physical isolation in restricted environment, dedicated lines of communication) help mitigate the risk of these vulnerabilities.

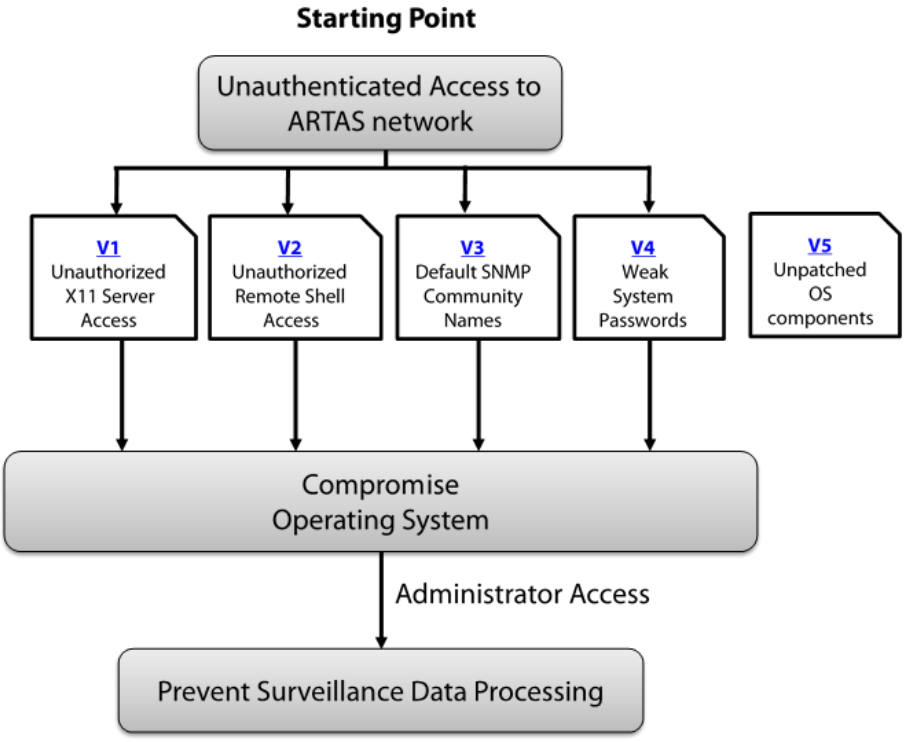

Figure 3 OS attack path

2.3. Attack on ARTAS application

Following the path of trying to compromise the ARTAS application, it was not possible to impact the ARTAS application, thanks to properly employed practices. See Figure 4.

Two main tactics were employed during this step:

1) Protocol Fuzzing: Plain and smart fuzzing was employed to ASTERIX fields trying to generate exceptions and potentially crash the ARTAS application.
2) Malicious Messages: Crafted ASTERIX messages specifically made to circumvent the protocol logic [12].

In both tactics, the ARTAS application handled the messages robustly and in an expected way; this means that the ARTAS application did not crash nor displayed any unexpected behaviour.

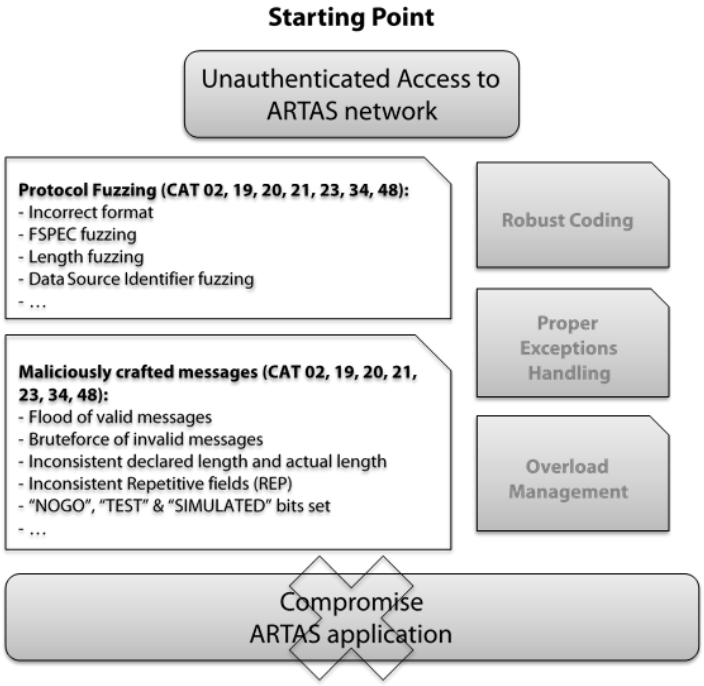

Figure 4 Application attack path

2.3. Attack on ASTERIX protocol

As known, the ASTERIX protocol does not offer any security mechanisms to ensure data source authenticity, data integrity, etc. [5] As such, it is trivial to impersonate existing Sensors/Users or modify legitimate messages, once we are on the same network with ARTAS [6].

Therefore, it was possible to degrade the status of existing, functional Sensors on ARTAS leading to the disappearance of the tracks reported by these Sensors, as well as to introduce fake tracks and flood the Air Situation Picture [7][8].

2.4. Recommendations

The following actions were recommending in order of priority, in order to further improve the security of the ARTAS System:

1) Operating System of ARTAS servers should be hardened:
   a. Services should use authentication and authorization mechanisms.

   b. Unencrypted protocols should be substituted by more secure ones.
   c. SNMP community strings should have a high complexity.
   d. Passwords should have a high complexity.
   e. Critical patches should be applied
   f. Unused services or components should be removed from the Operating System
2) Source authenticity and data integrity should be ensured in ASTERIX by other means/protocols (VPN tunnel, leased line, etc.).
3) Proper ARTAS architecture (isolation, secure line with Sensors, etc.) guidelines should be distributed to all ARTAS users.

3. RECENT IMPROVMENTS

Despite the fact that the ARTAS system is "air gapped" from the other networks, it is not possible to relay solely on this security measure anymore and additional techniques to protect the system should be applied. EUROCONTROL as the supplier of the system has taken into account the results of the assessment and the next version of ARTAS (version V9.0.0.0) which will be released at the turn of 2019/2020 will bring several security improvements. It is focusing mainly on the protection against the possibility to compromise the Operating System.

First of all, ARTAS V9.0.0.0 is based on the newest (at the time of the development) Operation System (Oracle Linux 7.5) which was stripped down to the minimum of necessary packages in order to minimise the "attack surface".

The biggest security improvement will be the use of the secure shell "ssh" connection instead of the legacy "rsh". Additionally, in default configuration, it denies the login of the "superuser".

It also utilizes the default Linux firewall (iptables), though due to the complexity of each ANSP's environment, there are no common firewall rules and the configuration of the firewall is left to the final user.

4. CONCLUSION

The article describes very current topic of security enhancements for ATM systems. It points out that current cyber security is achieved at the perimeter of the ATC environment. Many of the surveillance processing systems like ARTAS, didn't consider the cyber security during the design stage. Therefore, it is being implemented afterwards which has a significant impact on the costs [9].

ARTAS contains some critical vulnerabilities, allowing more freedom to the operators but also easy access to an attacker, that are mitigated by the fact that ARTAS systems should be isolated and restricted in a secure architecture. Every ANSP's implementation of ARTAS though, may be different, despite the recommendation to have ARTAS system installed in an isolated environment. Therefore, EUROCONTROL has resolved most critical vulnerabilities pointed out by the assessment in the upcoming version of ARTAS system.

References

[1] Industry Consultation Body #57, Position Paper on Regulatory Response to ATM Cyber-Security [Online]. Available at: https://ec.europa.eu/transport/sites/transport/files/modes/air/single_european_sky/doc/20150910_icb_position_on_regulatory_response_to_atm_cybersecurity.pdf.

[2] EUROCONTROL, 2018 ARTAS Air traffic management surveillance tracker and server[Online] Available at: https://www.eurocontrol.int/product/air-traffic-management-surveillance-tracker-and-server#implementation-status.

[3] 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
[4] Dzunda, M.; Kotianova, N.: The accuracy of relative navigation system. Conference: International Conference on Engineering Science and Production Management (ESPM) Location: SLOVAKIA Date: APR 16-17, 2015, Pages: 369-375, Published: 2016
[5] JANČÍK, M., DE HAAN, J. & JONÁŠ, P., 2019. Security Enhancements of the Surveillance Data Exchange Protocol "ASTERIX." DEStech Transactions on Computer Science and Engineering, (cscbd). Available at: http://dx.doi.org/10.12783/dtcse/cscbd2019/30009.
[6] 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: JAN 24-25, 2016, Pages: 290-294
[7] Dzunda, Milan; Kotianova, Natalia : Selected Aspects of Applying Communication Technology to Air Transportation. Conference: International Conference on Computer Science and Information Engineering (CSIE) Location: Bangkok, THAILAND Date: JUN 28-29, 2015, Pages: 1-7
[8] 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
[9] Džunda, M., Dzurovcin, P., Cekanova, D.: Operational economic aspects of warning collision systems for helicopters. Transport Means - Proceedings of the International Conference, 2018-October, pp. 1151-1155
[10] Galanda, J.: *Informačné technológie v manažmente I, Narušenie a ochrana informačného systému*. Kosice: Technical University of Kosice. 2017. 96 p. ISBN 978-80-553-2693-1.
[11] Galanda, J.: *Informačné technológie v manažmente II, Počítačové infiltrácie a ochrana dát v informačnom systéme*. Košice: Technical University of Kosice. 2018. 86 p. ISBN 978-80-553-3234-5.
[12] Džunda, M., Cséfalvay, Z.: Selected methods of ultra-wide radar signal processing. Marine Navigation and Safety of Sea Transportation: Advances in Marine Navigation. TRANSNAV 2013, pp. 239-242

Received 08, 2019, accepted 12,2019