Engage

At the core of the Engage KTN is the definition of various thematic challenges: new ideas suggested by the research community, not already included within the scope of an existing SESAR project. They are developed along with the ATM concepts roadmap and complementarily with some of the network's PhDs and theses.

Thematic challenge 1

Vulnerabilities and global security of the CNS/ATM system

Edition 4.0, April 2019

This is an evolving document that summarises the key concepts (and, later, findings) for thematic challenge 1.

Abstract

CNS/ATM components (e.g., ADS-B, SWIM, datalink, Asterix) of the current and future air transport system present vulnerabilities that could be used to perform an 'attack'. Further investigations are necessary to mitigate these vulnerabilities, moving towards a cyber-resilient system, fully characterising ATM data, its confidentiality, integrity and availability requirements. A better understanding of the safety-security trade-off is required. Additional security assessments for legacy systems are also needed to identify possible mitigating controls in order to improve cyber-resilience without having to replace and refit. Future systems security by design is essential: a new generation of systems architectures and applications should be explored to ensure confidentiality, cyber-resilience, fault tolerance, scalability, efficiency, flexibility and trust among data owners. Collaborative, security-related information exchange is essential to all actors in aviation. This is specially challenging in a multi-stakeholder, multi-system environment such as ATM, where confidentiality and trust are key.

Description of challenge

Data science applications are revolutionising many industries, including aviation. The increasing availability of data, coming from an increasingly sensorised and communicating sector is multiplying the opportunities of delivering data and information-based solutions to diverse challenges, including fuel efficiency, safety, predictability and crew training. However, this is also opening new vulnerabilities or hazards that need to be faced, as declared by the Industry Consultation Body (2017) in its information paper, noting that the increasing reliance on inter-connected ATM systems, services and technologies increases the risk of cyberattacks.

Aviation stakeholders, airlines, airports, and air navigation service providers all operate different information management systems for their operational purposes. This generates a complex, multi-stakeholder, multi-system environment where the global security of the system architecture needs to be ensured and its cyber-resilience needs to be further reinforced through a combination of organisational, procedural and technological elements (Everdij *et al*., 2016). The reliability of the information displayed and used by ATM/CNS components is crucial to ensure the safe operation of a flight. Different ATM systems (e.g. ADS-B, datalink, SWIM, Asterix) are vulnerable to certain attacks (some of which might still be unknown), such as: corrupting, through false instructions or information, aeronautical communications broadcast in known frequencies (Strohmeier *et al*., 2015); ADS-B false-aircraft transmissions – so-called false data injection attacks (FDIA; e.g. see Cretin *et al*., 2018); and, attacking key infrastructure element such as SWIM (system wide information management; e.g. see Everdij *et al*., 2016).

Considering the growing importance of communications, information and data sharing among ATM stakeholders, systems and components, it is necessary to ensure adequate protection against these and future potential attacks. Considering current global threats, it is pertinent to perform an initial security assessment of the elements supporting air navigation as well as their relationships, in order to identify its vulnerabilities. The collaboration of the different stakeholders plays a crucial role in achieving this objective, as highlighted by the ICB in its information paper (Industry Consultation Body, 2017), where sharing information about previous attacks and effective mitigations are considered a necessary step to protect the industry from future attacks. A European holistic, coherent, affordable and adaptable response that first understands the risks and then establishes mitigation measures is needed. The risk assessment should consider the potential impact of additional security measures to avoid unwanted effects regarding safety (e.g. TCAS encryption). On the other hand, it is necessary to apply controls to existing aviation and air traffic systems to detect exposure to attacks and make them cybersecure without having to replace and refit. Certification, legal and liability issues should also be taken into account. Identifying the vulnerabilities and anticipating potential risks should then be used to design adequate mitigation actions and procedures that may imply certain changes in the system.

In a growing environment of data-driven applications (machine learning, artificial intelligence, data science, etc.) likely capable of further improving aviation performance, we need innovative data-sharing architectures capable of connecting and providing access to distributed data while preserving data privacy. The optimal data-sharing framework for a multi-stakeholder, multi-systems system like ATM, should be built on data-owners' trust, placing data privacy at the heart of its architecture. The application of innovative, secure, distributed architectures, need to be explored in the aviation domain as a potential path to ensure trust from both the technical and data usage/protocol perspectives. Further studies should also analyse the use of advanced, secure computing functions for privacy-preserving applications built over distributed applications.

The information and communication technologies sector has made significant progress in this respect and, in particular, in the cybersecurity domain, which could be transferred to the aviation industry where several initiatives have also been launched. This previous work should serve as a basis for future research in the field. The SESAR cybersecurity strategy and framework study (SESAR, 2015), in particular, provides a European framework enabling the application of an aviation security maturity model to define the roadmap towards fully secured aviation. Challenges covered therein are: bridging the gap between security risk management and the system-of-systems architecture (EATMA); strengthening cyber-resilience by linking with operational contingency; and, assessing different architectural options from a security perspective.

The CANSO *Cyber Security and Risk Assessment Guide* provides an overview of the threats and risks, including considerations for managing them and suggestions for a cybersecurity programme (CANSO, 2014). In addition, a number of workshops and research projects have been organised around this topic, helping to progress beyond the state of the art, foster the debate and promote the creation of an associated community. The following (non-exhaustive) list collects some of the most relevant activities.

> The EUROCONTROL ART workshop on cybersecurity (EUROCONTROL, 2016) focused on providing recommendations to foster progress in the field, covering regulatory, liability, validation, human and organisational aspects, including cooperation and harmonisation with other non-EU programmes.
> EASA and EUROCAE (2017) organised a workshop on technical standards to initiate the discussion about future rule-making and standardisation for cybersecurity in aviation.
> The GAMMA project (2017) developed a new vision, representing a concrete proposal for the day-to-day operation of air traffic management security. The ATM security solution proposed by GAMMA builds on the principles and concepts related to security management in a collaborative, multi-stakeholder environment, while maintaining a strong link with the current international and European legal frameworks, and the constraints imposed by national sovereignty issues.
> The European Strategic Coordination Platform (2017) on cybersecurity in aviation, organised by EASA, accepted a declaration which "called upon the European Commission and the European Aviation Safety Agency to develop and adopt Implementing Regulations addressing Cybersecurity in Aviation with harmonised common objectives but tailored requirements for subjects and sub-sectors, assuring commensurate responses to risks, called on airports, ground handling operators, maintenance organisations, air navigation service providers to develop information security management systems in accordance with specific procedures and appropriate standards, recommended to harmonise the security risk assessment methodologies, recognised that cybersecurity is an interdisciplinary problem in transport that has its challenges in aviation, but also in shipping, rail and road transport, called upon a stronger partnership between regulators, operators, service providers, and manufacturing industry, in particular within the ESCP, where EASA welcomes and supports the Industry to come with standards."

Making the most of the latest progress achieved in previous and on-going activities, this thematic challenge aims to pave the way towards a privacy-preserving, cyber-resilient, fault-tolerant and trustworthy system of systems, with all layers ensuring the integrity and availability of aeronautical data.

Update from consultation

In order to propose more concrete lines of potential research activities on the topic, an internal consultation was performed involving Engage partners and Thematic Challenge 1 proposers. The result of this exercise is presented in the following lines and will be complemented by a thematic workshop (to take place in Spring 2019).

From the human and organizational perspective, the growing potential impact of the described cyber threats require the cooperation and adaptation of mental models within the sector. Stakeholders involved in aviation and air transportation, and more specially those directly interacting with the systems and basing his operations on them, need to be trained and prepared to understand and face the threads.

From the technological side, the complex, multi-stakeholder, multi-system environment that is developed in the CNS/ATM system, require to update software and firmware of IT components in order to fix security vulnerabilities of any critical infrastructure. The problem of ensuring that vendors will indeed guarantee development and delivery of security upgrades and security patches for 10 years or more will soon become of crucial importance. This is currently unsolved and involves several difficult issues: technical, economic and legal. These difficulties include either how to upgrade each component while ensuring capability with all other parts, or how to guarantee that this activity is economically sustainable over a long period. Taking into consideration the risks involved in the IT supply chain is an extremely hard problem. Moreover, the legal frameworks necessary for providing concrete operational guidelines suitable for these novel forms of

dependence are often still excessively vague. Assessing and managing these hazards is rapidly becoming and inescapable necessity in safety critical systems.

Focusing on the crucial security analysis and strategic protocols that are needed to mitigate the system's vulnerabilities, there is the necessity on analysing whether or not protocols contain weaknesses themselves or protocols scale to the new trust mechanisms required (i.e. do they contain the required security mechanism, or the ability to flexibly adopt new security mechanisms?). A deeper study on the security analysis of aviation specific protocol implementations has to be carried out, especially for the case of a common software library used across vendors to implement a protocol specification, to know the security vulnerabilities content that these products could expose.

To move to the managed service provision of surveillance data, such as space based ADS-B, introduces the need for service suppliers to provide adequate assurance that the data is secure. Models applied have to ensure data integrity while considering security quality to data source from multiple parties. A greater degree of technical integration and sharing data is also added with the intention of rationalization traditional radar information and the utilization of layers of newer surveillance technologies to advance the capability. This leads to the requirement of tightly considered security of the information, leading to the difficulty on how to constrained the data accessibility with the reduction of precision that this action involves.

Lastly, SESAR has progressed some work, so it is important to understand and know what is in future scope to avoid unnecessary overlapping between these two research lines. To achieve this, it is worth being clear about work progress, to later explore areas that have a low maturity level.

The following have been identified as *example* ideas for potential further exploration:

1. Perform an initial security assessment of the elements supporting air navigation as well as their relationships, in order to identify its vulnerabilities and to ensure adequate protection against future potential attacks and current global threats.
2. Apply controls to existing aviation and air traffic systems to detect exposure to attacks and make them cyber secure without having to replace and refit. Certification, legal and liability issues should be taken into account.
3. Innovate data-sharing architectures capable of connecting and providing access to distributed data while preserving privacy.
4. Adapt mental models within the sector to prepare operators to understand and manage cyber threats.
5. Requirement of updating software and firmware of IT components in order to fix security vulnerabilities of any critical infrastructure.
6. Deeper study on the security analysis of aviation specific protocol implementations (vulnerabilities, trust, software library).

Workshop conclusions

Summary of the research ideas that emerged from the workshop:

- The relative importance of confidentiality, integrity, and availability depends on the information in question and in the application area. For personal information on ANSP staff, or for maintaining the anonymity of state flights, maintaining confidentiality is indeed important. There are research opportunities in applying encryption methodologies to overcome this challenge without compromising safety. However, for ephemeral operational data such as tracks, integrity and availability are probably more important and their assessment needs to be further investigated.
- Future research projects will require cooperation between multiple transport modes and other sectors to obtain funding. Reducing environmental impact will be a key requirement, as well as the

provision of evidence that core components are close to industrialisation. Contributing to the streamlining of safe and secure transport is also key.

- To maintain safety levels, current ATM/CNS systems are subject to rigorous change-management procedures to ensure that required system updates do not have an adverse impact on the reliability of the system. However, if new security vulnerabilities are identified in an ATM/CNS system, there is pressure to update the system as quickly as possible to prevent it from being subject to attack. New approaches are required to develop systems which are capable of addressing these conflicting demands while maintaining resilience. Just as an example, the application of AI algorithms could be explored to proactively detect patterns and mitigate attacks.
- New developments in screening, monitoring, and tracking may potentially breach accepted norms for ethics, privacy, societal acceptance, and could be in breach of the regulatory framework. Consideration of such non-technical potential issues in advance of embarking on such programmes would be prudent. Engaging the whole society would help building cyber-resilient culture. Security governance framework needed to establish the common policies, legal aspects and procedures for all stakeholders to collaborate as a resilient ecosystem.
- The secure sharing of information related to security between ATM/CNS stakeholders is required at many levels. Examples include: post-incident forensics; real-time alerting of security incidents to connected partners; threats & vulnerabilities; lessons learned, for example detection, response and recovery methods; … enhancing these capabilities is necessary.
- Assuring the security of the CNS/ATM systems requires shorter implementation times and updates/upgrades. Safety regulations are therefore challenged to face cybersecurity needs (e.g. patch management). The ability to rapidly patch vulnerabilities will be necessary when aircraft become more connected, which implies further development in certification processes of certified software (ED12-C). The requirements for certification of safety-critical systems should also include best practices from the security community.
- Progress in security risks assessment is required (including the development of indicators for key risks) as a first step in understanding, controlling and preventing the vulnerabilities of the systems. Adequate training for operators should be provided in order to increase the awareness and develop operational procedures for risks identification and reaction.
- New open models to enhance security should be developed in opposite to the more traditional approach of security by obscurity. Aviation could learn from other sectors (e.g. banking) in order to overcome national sensitivity and confidentiality across boards to the benefit of a collaborative security culture.

References

CANSO, 2014. CANSO Cyber Security and Risk Assessment Guide. https://www.canso.org/canso-cyber-security-and-risk-assessment-guide

Cretin A, Legeard B, Peureux F, Vernotte A, 2018. Increasing the Resilience of ATC systems against False Data Injection Attacks using DSL-based Testing. 8th International Conference for Research in Air Transportation – ICRAT 2018, Castelldefels, Spain.

EASA, EUROCAE, 2017. Workshop on Cybersecurity in Aviation, 31 May 2017, Brussels. https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20workshop%20Report%20-%20final.pdf

EUROCONTROL, 2016. Agency Research Team Workshop 'ATM Security and Cybersecurity' – 23rd March 2016, ENAC, Toulouse, France https://www.eurocontrol.int/events/agency-research-team-workshop-atm-security-and-cybersecurity

European Strategic Coordination Platform, 2017. https://www.easa.europa.eu/newsroom-and-events/news/high-level-conference-cybersecurity-civil-aviation-krakow-declaration

Everdij M, Gijsen B, Smulders A, Verhoogt T, Wiegers R, 2016. Cyber-security management of ATM services: are we ready for the future? Aviation security international, June, pp. 34-36.

GAMMA project, 2017. - Global ATM Security Management Project, European Union's Seventh research and innovation Framework Programme. http://www.gamma-project.eu.

Industry Consultation Body, 2017. Information paper on Industry Developments in ATM CyberSecurity, 3 Nov 2017. http://www.icb-portal.eu/phocadownload/TSG_Positions/Industry%20Developments%20in%20ATM%20Cyber-Security%202017%20Issue.pdf

SESAR, 2015. SESAR Strategy and Management Framework Study for Information Cyber-Security, September 2015. https://www.sesarju.eu/sites/default/files/documents/news/SESAR_Strategy_and_Management_Framework_Study_for_Information_cybesecurity_FINAL.pdf

Strohmeier M, Lenders V, Martinovic I, 2015. On the Security of the Automatic Dependent Surveillance-Broadcast Protocol. IEEE Communications Surveys & Tutorials, 17(2), pp. 1066 – 1087.