Collaborative cyber security management framework

Executive summary

While the ATM industry has been addressing cyber security since the mid-2000s, progress has been faster in the more operational and tactical side of security than the more strategic, management side. Within the safety domain, safety management systems have been continuously researched and developed, through practical experience and extensive collaboration. The practice of security derives from a 'need to know' approach, where information sharing is done sparingly, and collaboration is light. A recent World Economic Forum (WEF) study comments on the limited participation to the Aviation ISAC, where the need is for a collaborative approach from all actors in the aviation value chain, building on the strong history of safety management. The WEF study also emphasises the need for systemic risk assessment. This sets the context for this project, which addresses several themes in security management, centred around collaboration and risk.

The project has addressed a new concept of 'collaborative cyber security management' and to do this connects several different strands of work: risk, architecture and collaboration. Two initiatives in particular have provided inspiration for this project:

- **ED-201**: EUROCAE's ED-201 'Aeronautical Information System Security (AISS) Framework Guidance'. This provides guidance for different aviation organisations to cooperate on aeronautical information systems security (AISS).
- **STORM**: EASA's Shared Trans-Organisational Risk Management (STORM). This is a framework under development by EASA and EUROCONTROL, to support sharing of information as foreseen in ED-201. It requires methods to harmonise risk-assessment and share appropriate outputs, which map to organisations' functions and the interfaces between them.

The project addressed the following research questions:

1. How could ATM stakeholders collaborate better through productivity tools?
2. How can we evolve risk methods in ATM from purely qualitative to quantitative methods that support better use of information?
3. How can we connect risk management to architecture in a simpler, less resource intensive way?

The research was organised into two main work packages:

- WP1 CONOPS Development: covering the main elements of the project: collaboration, risk and architecture integration.
- WP2 Prototype Development: using an agile approach with regular iterations between the developing CONOPS and findings from the prototyping.

The project consulted ATM industry experts, particularly those knowledgeable with EASA's STORM concept and ED-201 guidance on Aeronautical Information Systems Security (AISS).

The risk aspects of the project focused firstly on quantification and secondly on exploiting quantified methods. This enabled the project to introduce a probabilistic graphical model (PGM) representation, using Bayesian Networks.

Prototyping was a key component of the project as it supported development of the CONOPS, which allowed the team to assess how productivity tools can support greater collaboration and improve the effectiveness and efficiency of security management. The prototyping was then done in three parts:

1. A prototype for risk management within an organisation or trusted community of practice, such as a SESAR, extended to quantitative risk assessment.
2. A prototype information broker to exchange information between risk assessments.
3. Bayesian network modelling: proof of concept modelling for future adaptation to STORM 1.

Functional architecture for the prototyping was developed in MS PowerPoint and LucidChart. The main prototyping was developed on a Node.JS platform programmed in the JavaScript language, based on a MySQL database.

The results of the project were assessed within the project team, with BULATSA providing an internal review as security practitioners. Overall, the project provided insight and emerging methods and tools that should improve cyber security management in ATM. Specifically, the project has:

a) **Identified how ATM stakeholders could enhance their collaboration on cyber security through productivity tools**. The concept of operation has considered the factors that can encourage or discourage exchange of information and proposes a way of collaborative working, which also requires productivity tools to support information exchange and increase efficiency.

b) **Evolved risk methods in ATM from purely qualitative to quantitative methods**. The project has also provided insight into the use of quantitative methods in risk assessment and adapted the SecRAM methodology to this. We also conclude that quantification does not add significant overhead to risk assessment, and there is an opportunity for partners to share, for example, impact assessments of the loss of CIA to primary assets. Quantifying the results of risk assessment may also benefit information sharing, as the outputs of different partners are comparable, even if the underlying risk assessment methodology is different. This said, harmonisation of methodology, such as through ISO 27005 or SecRAM, is likely to have a bigger impact on sharing risk management information.

c) **Identified how to connect risk management to architecture in a simpler, less resource intensive way**. The creation of a 'light' architecting approach has shown the benefits of visualising primary and supporting assets as functional diagrams. Although the prototyping was fairly simple, the visualisation provides user benefits in terms of appreciating the overall system. This light approach means that risk assessment and enterprise architecture could be done more in parallel in the SESAR processes without a need for resource intensive architecting to proceed first. This makes the process easier to do for early stage development of SESAR Solutions at V1 and V2 validation stages where Solution architecture may be incomplete.

This project has received funding from the SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287.