1st OPTICS2 Workshop

Aviation cybersecurity

Insights from the 1st Workshop

Those cyber-attacks which have already occurred are early warnings, representing the 'beginning of the curve'. There is still time to react, and get ahead of the cyber-threat curve, but the necessary work needs to start now!

5-6 June 2018

EASA, Cologne | Germany

Insights from the 1st Workshop

Aviation cybersecurity

What's around the corner, and are we ready for it?

Cyberattacks are relatively low cost and low risk for the perpetrator, but can be very high cost for the targeted organisation and society. In order to address this phenomenon, OPTICS2 brought together more than 50 experts from all aviation domains to consider both existing and potential future cyber risks, and identify a top list of both urgent and mid-term research required to maintain a safe and secure air transport system today, and in the future.

Luc Tytgat, Strategy and Safety Management Director, opened the event. Luc highlighted the importance for EASA of hosting this workshop, as EASA is strongly focused on emerging aviation cybersecurity risks. It is crucial for EASA to influence research prioritisation in view of future regulation, and OPTICS2 can help define these priorities on the basis of the knowledge of its network of experts.

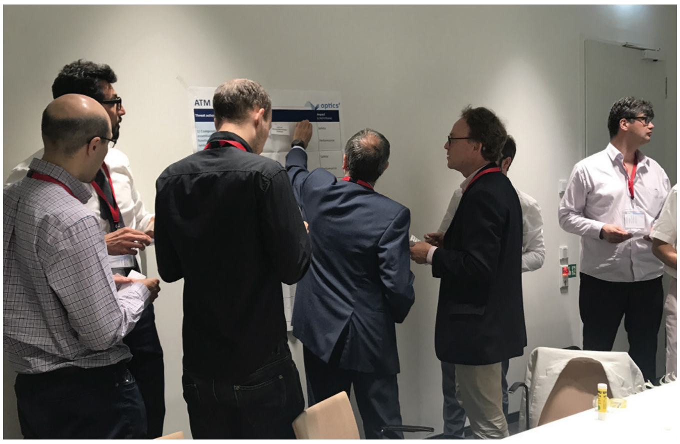
Pablo Pérez-Illana, Directorate General for Research and Innovation of the European Commission, pointed out the exponential growth of data from all sectors of the global air fleet, which in 10 years will amount to 100 Exabytes per year. Pablo noted that cyberattacks have already happened (e.g. Perth airport in Dec 2017, some frequent flyer schemes from Airlines, etc.), raising issues of confidentiality. Other issues with integrity and availability of services have also appeared. Research and Innovation (R&I) can underpin a more secure digital revolution, a better understanding and mitigation of risks, and also lead to better regulation. Cybersecurity is becoming more and more critical for aviation. Pablo concluded by reminding that aviation should exploit synergies with other advanced sectors to strengthen its cybersecurity, as offered in EU programmes such as Connecting Europe Facility and Horizon 2020 (e.g. Security & ICT calls for proposals).

Marouan Chida, SESAR JU's Digital Transformation and Innovation Manager, focused his presentation on the need for cyber-resilient architecture. He provided three research priorities, consisting of defining best practices to implement security by design, creating a trust framework, and applying the most advanced technologies to stay ahead of the game.

Simone Pozzi, Deep Blue CEO and OPTICS2 Project Coordinator, provided a brief overview on the OPTICS2 Project, and illustrated the workshop goal, objectives and approach. The workshop combined high level speeches with two guided workshop sessions aimed at discussing current and emerging cybersecurity threats, developing potential threat scenarios and thus identifying research priorities for aviation cybersecurity.

Cyrille Rosay and **Jean Paul Moreaux,** EASA Cybersecurity experts, presented the EASA Cybersecurity roadmap, developed in November 2015. Since then, under EASA's umbrella, a number of high-level conferences on

Insights from the 1st Workshop



cybersecurity in civil aviation have taken place, and the ECCSA (European Centre for Cybersecurity in Aviation) and ESCP (European Strategic Coordination Platform) have been established. Believing that there are strong interdependencies between safety and security, EASA has fully taken into account cybersecurity threats in the development of the European Plan for Aviation Safety (EPAS) 2018-22. EASA is also collaborating with ICAO on the implementation of an international System Wide Information Management (SWIM) system.

Giuliano D'Auria, Leonardo, presented the GAMMA (Global ATM Security Management) Project. GAMMA addressed ATM threats and vulnerabilities due, for instance, to the increased reliance on distributed enterprise computing and the automated flow of information across ground and airborne networks. The project has developed an ATM Security Management platform prototype, aimed at managing security at local, national and European levels.

Chris Johnson, University of Glasgow, focussed on defensive measures which can be undertaken to neutralise current cybersecurity threats, such as ensuring staff competence, and performing cybersecurity risk assessment. Chris illustrated the importance of carrying out penetration tests for airborne systems and highlighted how complacency is one of the major issues for cybersecurity, leading e.g. to shared passwords within organisations, and sensitive material and classified documents on sale on eBay.

After lunch, the 1st workshop session took place, aiming at identifying the major threat actions for the three aviation segments (ATM, airborne, and airport) and developing potential threat action scenarios (see Box 1 on the right).

BOX 1 WORKSHOP SESSION 1

EXPLORING CYBERSECURITY THREATS

Format: 3 mixed-groups representing the three aviation segments: Air Traffic Management, Airborne, Airport.

Goal: to identify the most relevant cybersecurity **threat actions** for each aviation segment.

Results: the outcome of each group is summarised below, listing the selected **threat actions** and further detailing them by describing potential threat action scenarios.

The definition of each threat action is available at the end of BOX 1.

Compromise of essential functions and systems

Corrupted radar picture on controller working position; GNSS spoofing during aircraft approach.

Air Traffic Management | Airborne | Airport

Loss or compromise of communication services

Jamming or spoofing of voice communications between aircraft and air traffic control.

Air Traffic Management | Airborne

Loss of essential supporting services

Compromise of power and water supplies at airport.

Airport

Criminal actions

State-sponsored cyber-attack on airport systems.

Airport

Threat Action Description

Compromise of essential functions and systems:
A hostile act intended to cause denial of services and loss of essential systems due to corruption of data or operation or physical damage.

Unauthorized access:
An action resulting in unapproved physical or digital access to infrastructure, vehicles, systems and border security.

Loss or compromise of communication services:
A hostile act intended to cause loss of communication services such as jamming and spoofing of systems and services.

Loss of essential supporting services:
A hostile act intended to disrupt and/or destroy essential serv¬ices such as power, energy, water.

Airborne threats:
Actions relating directly to an air vehicle such as conventional hijack, MANPADS, using the vehicle as weapon.

Criminal actions:
Actions including kidnapping, bribery, extortion, fraud, blackmail, sale of stolen information, smuggling and contraband, data and intellectual property theft.

optics²

Insights from the 1st Workshop

Kai Jansen, Ruhr-University Bochum, opened with an example of a cybersecurity issue in a transport mode other than aviation. Kai illustrated how crowdsourcing can be used to detect and localise GPS Spoofing Attacks, using the case study of a GPS spoofing aimed at a ship cruising the Black Sea in June 2017. Detecting the exact location of the spoofing device was an issue, and Kai presented a technique allowing faster detection and more precise location of such devices.

Angela Vozella, CIRA, illustrated the OPTICS2 Assessment Methodology. Angela focused on the twofold approach adopted by OPTICS2, aimed at complementing the R&I project assessment performed by the OPTICS2 experts (bottom-up) with expert contributions collected via workshops and ad-hoc consultations.

Paolo Giorgini, Trento University, presented the PACAS (Participatory Architectural Change mAnagement in ATM Systems) Project in order to show how the OPTICS2 methodology applies in practice. PACAS is a Horizon 2020 project addressing both safety and security aimed to better understand, model and analyse changes at different layers of the ATM system to support change management, while capturing how architectural and design choices influence the overall system. PACAS relies on three main pillars: impact propagation techniques, a gamified platform, and domain-specific modelling languages. Besides providing an overview on the project, Paolo showed the results of the assessment performed by the OPTICS2 experts on PACAS.

Juan Caballero, IMDEA Software Institute, opened day 2 providing an overview of the IMDEA malware network communication measurement, which lasted almost 5 years. The analysis covered both malware and PUP (Potentially Unwanted Program). Juan explained how malware is often included in remote attacks and that it is the product of a hacker, while PUP is managed by companies trying to sell their products (unwanted ads for virus protection, etc.) and now dominates over malware attacks. Recently, hosting providers (cloud-based) have been attacked instead of individual machines.

Taha Cherfia, FORTISS, reinforced the necessity of knowledge exchange from different transport fields, as cyberattacks are now affecting all modes: maritime, automobile, aviation and rail. Taha presented the CYRAIL Project, which studied cybersecurity threats targeting railway infrastructures. The main issues comprise high implementation costs, a “security by afterthought” approach as opposed to “security by design”, the lack of cybersecurity standards and certifications for railways, and the lack of security awareness and expertise.

Giovanni Gamba, Qascom, presented the IACT (Impact Assessment of Cybersecurity Threats) Project conducted for EASA. The primary targets of the project were to identify and prioritise threats to critical aircraft systems as well as to build a comprehensive knowledge base of the safety impact of these threats on flight operations. The project contributed to consolidate methods and techniques for risk assessment and mitigation using flight procedures.

Francesco di Maio, Head of Cybersecurity and Risk Management at ENAV and CANSO Security Chair, conveyed ENAV’s view on security challenges of ATM digital era 2.0. Francesco reminded the audience that safety and security are bridged, and highlighted cybersecurity issues relevant for aviation, such as the coexistence of different legacy systems currently in use, the arrival of new operational concepts (e.g. remote towers, drones, free routes, etc.), increasing interdependencies, and the need for more flexibility. Francesco stated that there was an urgent need of the aviation industry to assess the limits of the current systems in order to tackle these new threats.

The 2nd workshop session aimed at identifying the top cybersecurity research priorities for the total aviation system. Each group (ATM, Airborne, Airport)

identified the research topics associated to the threat action scenarios developed in the first session and selected the most relevant ones for the assigned aviation segment. The top research priorities were selected through plenary real-time voting (see Box 2 on the righ).

Clive Goodchild, BAE Systems, and **John Hird,** EUROCONTROL, closed the workshop providing a sneak peek on the OPTICS2 preliminary findings. John presented the methodology for the weighting of the Strategic Research and Innovation Agenda action elements, and presented the initial results from a pilot assessment, carried out by a cross-section of industry experts. All the attendees at the workshop were invited to contribute to this activity to further refine the results. Clive gave some insights into the State-of-the-Art of European Security R&I based on the initial results of the OPTICS2 assessment (39 projects assessed in Year 1). The topics on which research appears to be focused are System-wide security governance (Action Line 6.1), People management (7.1), and Secure flow management (9.2), while the ones poorly covered are Information management and sharing (8.4), Legal Framework (7.3), and Security radar (8.2). Furthermore, as yet there is no research on Horizon scanning (8.3) .

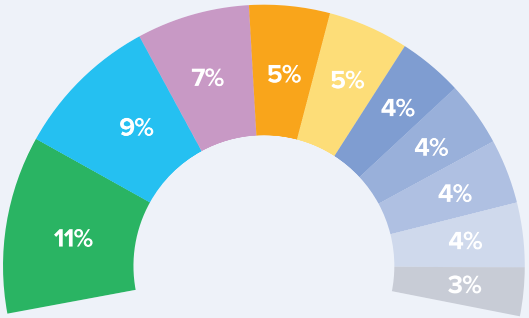
BOX 2 WORKSHOP SESSION 2

TOP RESEARCH PRIORITIES

Format: 3 mixed-groups (different composition comparing to session 1) representing the three aviation segments (ATM, Airborne, Airport), followed by plenary voting.

Goal: to select the top cybersecurity research priorities for the total aviation system.

Results: shown below.



- 🟩 Improving security culture and risk awareness (tools and techniques)
- 🟦 Security by design for the whole lifecycle
- 🟪 Safety and security integration
- 🟧 Maintaining security of a system throughout its whole lifecycle
- 🟨 Improved anomaly/intrusion detection
- ■ Improved cybersecurity situational awareness for incident management
- ■ Artificial intelligence systems for improved cybersecurity
- ■ Dynamic and Integrated Safety-Security Risk Management
- □ End-to-end authenticity supported by international regulations
- ■ Improved incident information sharing

optics²

Insights from the 1st Workshop

Beyond the filtering and post processing to establish a picture ,how can this be used for prevention ?
Mark as answered

Designed and produced by Deep Blue

Concluding comments

The OPTICS2 cybersecurity workshop held at EASA involved fifty experts from all sectors of aviation, and gave a clearer picture of the current state of aviation cybersecurity, the future challenges facing the industry, and the top research priorities to help protect aviation from cyber-threats now, and in the future.

Today, aviation is clearly at risk, and yet many segments of the industry lack robust counter-measures against cyber-threats. One of the speakers summed up the current state of affairs as **security as an after-thought, not by design.** The consensus was that sometimes even basic counter-measures and processes, and more generally security awareness, are not in place, even though cyber-defence knowledge and understanding of cyber-attack mechanisms and potential countermeasures is increasing all the time. A number of cyber-attacks have already occurred in aviation, seen by the experts as early warnings of what is to come, representing the 'beginning of the curve.' Clearly the challenge is to react now, and put counter-measures and security systems in place before attacks increase in frequency and/or severity.

As data and inter-connectivity increase in the industry, in line with societal and business trends, this represents both a challenge – since more interconnectivity can increase the 'capacity' for cyber-threats, as well as their novelty and severity – and an opportunity, if data can be harnessed to detect and neutralise anomalous system behaviour due to malware insertion, etc.

During the workshop, experts split into groups to determine the top threat priorities for each operational aviation segment (airborne, air traffic management, and airports), resulting in a matrix of top threats and impact scenarios (see inside this report), which should prove useful for those managing security in the industry, as well as for researchers, giving them concrete contexts to study.

The top ten aviation cybersecurity research priorities were identified by the expert participants. The clear winner was the need to develop a security culture across the industry, with heightened security awareness of all staff, supported by robust security processes and techniques. This is seen as necessary due to perceived complacency and lack of preparedness in the industry, as well as a lack of validation of existing security measures (e.g. via so-called 'penetration tests').

The next four research priorities relate to learning how to be secure by design, moving safety and security closer together so they can learn and leverage from each other, determining how to maintain the security of a system throughout its entire life-cycle, and developing improved detection means for anomalies and intrusions.

In summary, there is still time to react, and get ahead of the cyber-threat curve, but the necessary work needs to start now.

The OPTICS2 Team would like to thank all participants for their energy, enthusiasm and insight!