SATIE NEWSLETTER

APRIL 2021 ISSUE 2

INSIDE THE ISSUE

PROJECT CONTACT

Tim H. Stelkens-Kobsch
communication-satie@dlr.de

ONLINE LINKS

Twitter
SatieH2020

LinkedIn
showcase/satie-h2020

Website
satie-h2020.eu

Foreword

By Tim H. Stelkens-Kobsch, DLR, SATIE Project Coordinator

In this second issue of the SATIE newsletter, I am happy to introduce you to some important developments which have emerged from the project over the last few months, as well as the new challenges expected in 2021. The SATIE concept has been translated into a set of prototypes, which are interconnected to a holistic system and will be validated in the upcoming simulations and demonstrations in the first half of 2021. Results from SATIE are meanwhile being reflected in the various dissemination activities and publications performed in the last few months.

This newsletter opens with an article dedicated to the first Awareness Event of SATIE, which took place remotely on November 17th 2020 and which received high interest from a wide variety of stakeholders. It continues with a more detailed look at two of the scenarios, which SATIE implements to test its toolkit. Furthermore, you will find insight into one of our partner companies and the developments we have achieved in the dedicated work package which focuses on the detection and correlation of cyber and physical threats.

In order to provide an independent assessment on the systems and how the SATIE toolkit is suited to respond to the security challenges airports are facing, SATIE intends to rely on external users and experts. I therefore take the opportunity of this newsletter to welcome users, stakeholders, and security experts to engage actively with the project as it enters this crucial validation phase. This is your chance to become engaged as an active player in the validation of SATIE so please contact us (email: communication-satie@dlr.de) if you are willing to come onboard!

I hope this newsletter will further stimulate your interest in SATIE.

First SATIE Awareness Event

The SATIE Awareness Event took place on Tuesday, November 17th, 2020, as a remote conference. It hosted in total 71 participants, including guests from EDA, EASA, ENISA, DG JRC, DG HOME, DG Connect, EUROCONTROL, SESAR JU, other research institutes and industry partners. After invited presentations from Max Brandt (DG HOME), Wide Hogenhout (DG Connect) and Dimitra Liveri (ENISA), stressing the need of security and pointing out the challenges of policy making, the SATIE team presented an overview of past attacks and provided insight into the SATIE solutions.

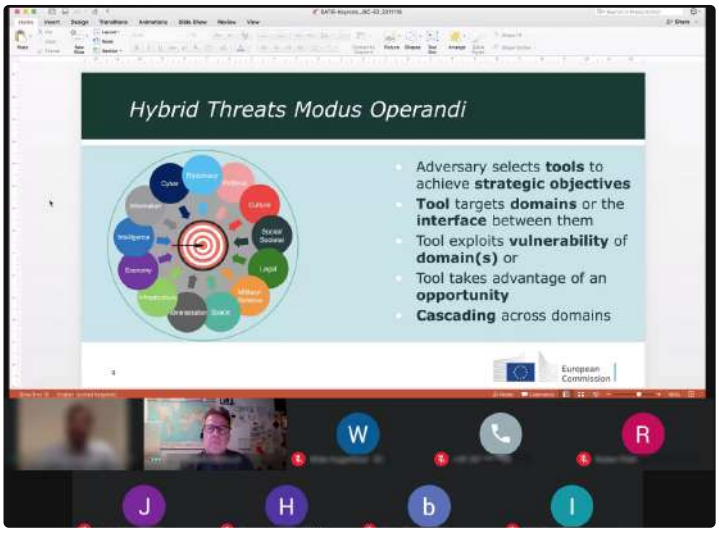
Selected SATIE tools, which are available to the Security Operation Centre (SOC) operators, were shortly introduced by the respective partners in a dedicated session. Thereafter, those tools were presented in the context of two SATIE scenarios. The scenarios were introduced with presentations and dedicated videos highliting the attack steps and where the benefits of the SATIE Solution lie.

The whole event can be seen as a great success attracting many external guests. Some of the general appreciation remarks were:

- "Very interesting conference."
- "Thank you very much for this experience it was a big pleasure to join you today!"
- "... amazing work!"

The discussions with the experts during the event provided valuable feedback that will be used to improve the tools.

Discussion headlines from the first Awareness Event



Hybrid Threats Modus Operandi from the Scenario #1

Presentation of Scenario #1

By David Lancelin, Airbus CyberSecurity

This threat scenario targets different Information Technology (IT) and Operational Technology (OT) systems of an airport. The scenario involves two unsuspecting cyber-attacks to gain enough information to carry out a subsequent physical attack and control the movement of people, thereby enabling further physical attacks. The mitigation of the two cyber-attacks also occupies the airport's security response teams. The distraction of relevant personnel increases the probability that the subsequent physical attacks end with a devastating impact. The attackers try to gain access to a central information system of the airport.

After gaining this access and remotely entering another system, the attackers have control over critical security measures. With the achieved accesses the attackers would be able to physically enter restricted areas and direct passengers as they want, therefore causing chaos throughout the airport.

This can then be used to start possibly devastating physical attacks. The SATIE solution allows responding to the threat by detecting suspicious access to IT systems thanks to a cyber threat detection system, the exploitation of vulnerabilities thanks to the integration of the Vulnerability Management System and by preventing unauthorized access to security restricted areas through the Unified Access Control system that performs a security cross-check between badge validation and facial recognition prior to allowing access to a restricted area. All of these security systems are connected to the Correlation Engine and monitored by the Security Operation Center, where security operators and analysts receive, process and assess security alerts within the Incident Management Portal. In order to analyze security alerts, they can rely on the Investigation Tool, which can find evidence of the causes of the attack. In case of a security incident that affects passengers or employees, the Impact Propagation Simulation triggers an agent-based simulation environment.

Thanks to this SATIE tool, the impact can be analyzed in a quantitative manner. In addition, it allows the visualization of the attack path in a network representation of the airport, making it possible to predict a possible propagation of a threat. Finally, the Crisis Alerting System shares the incident information and notifies the various stakeholders for coordinated security and safety responses.

Presentation of Scenario #5

By David Lancelin, Airbus CyberSecurity

This threat scenario targets the Air Traffic Management (ATM). The Air Traffic Controllers (ATCOs)/Apron Controllers are distracted due to a chain of cyber-attacks on the computer systems. A second attack is then performed to issue some fake clearances and movement advice to aircraft potentially causing collisions of aircraft full of passengers.

The scenario starts immediately with a physical attack by one intruder at the airport gaining access to servers. The attacker then performs scans to find and identify a server which provides core ATC services. With suitable tools, the attacker gains access to this server. Now that the attacker has found and has access to the server, he performs a cyber-attack against the services running on this server in order to degrade the services and to create chaos.

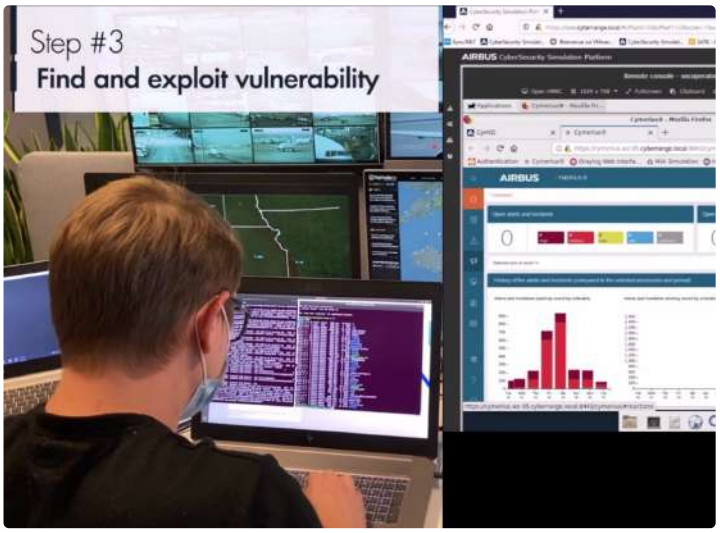
This also distracts the ATCOs as they try to determine why the system is not working. Then a second attacker can get on the appropriate radio frequency and falsely act as an ATCO to issue faked clearances to aircraft on the ground.

Physical intrusion into a restricted area as shown during the first SATIE Awareness Event

As the real ATCOs are currently distracted by the failed core services, the attacker can issue potentially dangerous clearances.

Thanks to the SATIE solution, and in particular to the Unified Access Control system, the physical intrusion in the technical cabinet is detected and monitored by the SOC. The system allows detecting criminals on alert watchlist via face detection. Similarly, a cyber threat detection system detects the cyber-attack against the ATM services and sends security alerts to the SOC.

In addition, the SATIE Secured ATM Services logs information to allow the Correlation Engine to detect a variety of cyber-attacks. Finally, the Traffic Management Intrusion and Compliance System detects aircraft route deviations, unauthorized speakers and aircraft conflicts in order to prevent any aircraft collision.



Cyber attacks to airport systems as presented at the first SATIE Awareness Event

Partner Profile - DGS Spa

By Matteo Mangini, DGS

DGS is a private group which operates in the ICT industry since 1997, providing high-tech, value-added business solutions, combining a strategic vision related to business goals, with a technology-based innovative soul.

From strategic consulting to infrastructure management, the group's offer is targeting Large Customers, covering the entire ICT value chain: planning, design, development, integration, implementation, and maintenance of complex infrastructures, based on all the major technologies on the market. Thanks to the high quality of services offered in Cyber Security and Digital Solutions fields, DGS has gained a prominent position in major public and private companies, consolidating its presence on the market in the areas: Energy & Utilities, Public Sector, Finance Services, Industry and Manufacturing.

The group today employs more than 950 professionals of high seniority, distributed among the locations in Rome (HQ), Turin, Sesto San Giovanni, Genoa, Savona, Naples, Foggia, Bari and Rende. The strength of the company is a well-integrated and certified team of professionals, formed over 20 years, able to combine skills in cybersecurity technologies (vulnerability assessments, penetration testing, network security, threat analysis, etc.) with Governance, Risk and Compliance methodologies and tools to protect organization's data.

DGS
BUILDING THE FUTURE

950+
EMPLOYEES

400+
CERTIFICATIONS

2
R&D LABS

9
OFFICES

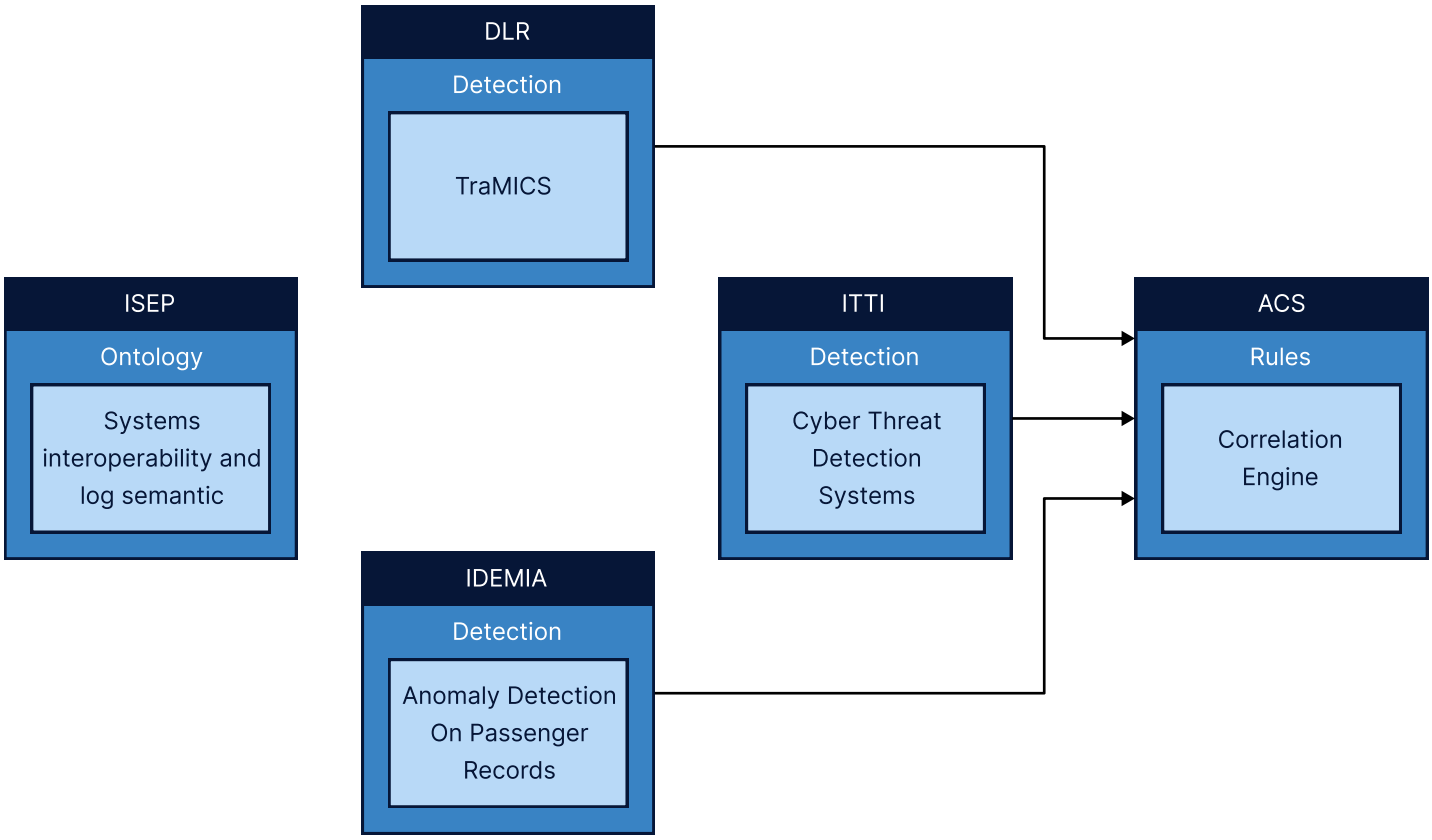
One of the outstanding elements for its security market is represented by RIS (Risk Integrated Service), a web-based Risk Assessment solution, implementing the DGS methodology in accordance with ISO31000. It was developed to help security consultants analyze, assess, evaluate, and manage risks related to assets, threats, and vulnerabilities within the company. Data gathered from the company's sites are integrated with information about the business and security guidelines to define cyber-physical risk scenarios. The RIS application offers management reviews, how risks can propagate throughout the organization, and treatment plans including highlighting which activities can best mitigate the identified risks.

Scan the QR code to view the video of the SATIE project

WP4 summary

By Thomas Oudin, Airbus CyberSecurity

WP4 is composed of the ontology, detection tools - Traffic Management Intrusion and Compliance System (TraMICS), Cyber Threat Detection Systems, Anomaly Detection On Passenger Records - and the Correlation Engine that receives events from all the SATIE detection tools (see Figure "Interrelations between WP4 tools")



Interrelations between WP4 tools

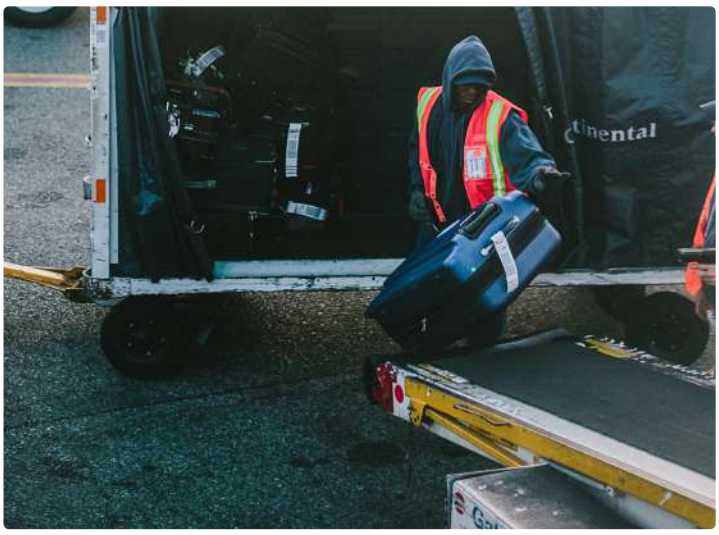
One of the goals of the SATIE project is to have a holistic cyber-physical view of airport security. Several systems are involved in this, and all of them must be able to communicate and understand each other. Thanks to the ontology the goal was reached, and the ontology bridges the gap between the airport security domain and cybersecurity solutions. All possible communications between SATIE's systems are clarified and described.

The first of the three detection tools is the TraMICS. Its goal is to improve spoofing detection on radio communication channels. TraMICS is able to detect unauthorized speakers, non-conformance of movements (for example route deviations - see figure "TraMICS showing a route deviation") conflicts and non-compliance to clearances. TraMICS is capable of examining stress in voices and will send alerts and the determined security situation indicator to the Correlation Engine. The second detection tools are the cyber threat detection systems. They are composed of ALCAD which detects anomalies using flow data, BP-IDS (Business Process-based Intrusion Detection System) which detects cyber threats in the baggage handling system including the baggage screening and the baggage sortation, and the Malware Analyser.

The goal of the third detection tool, Anomaly Detection On Passenger Records, is to improve detection of anomalies by extending the passenger threat to their baggage. The enrolment of the baggage will be at the time of check-in and the reference between passengers and their baggage will be shared. The baggage is authenticated (see figure "Checked baggage") to ensure it is not tampered during its lifetime in the airport. The system can also be used to rapidly find the owner of lost baggage to avoid disturbances in the airport.

The Correlation Engine receives events from all the SATIE detection tools, and with the creation of rules, it can correlate cyber-physical security events to raise alerts to SOC operators and assist in the investigation. Thanks to the Correlation Engine the correlations between different events can easily be identified.

TraMICS showing a route deviation



Checked baggage

Disclaimer: This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 832969. This output reflects the views only of the author(s), and the European Union cannot be held responsible for any use which may be made of the information contained therein.