NEWSLETTER | Issue n° 5 | September 2017

CONTENTS

EDITORIAL

As the GAMMA project draws to a close I am pleased to introduce you to this latest edition of the Newsletter. This issue includes an article describing the execution of the first integrated validation exercise. The demonstration applied the GAMMA Conops and the layered approach to managing security in Europe to the specific case of coordinated attacks. This scenario was successfully simulated by using a fully connected geo-distributed setup involving prototypes developed by several GAMMA partners.

The SMP prototype lies at the heart of this geo-distributed platform, enabling the sharing of security relevant information between the different levels of the GAMMA solution. While a general article on the SMP has already appeared in a previous issue of the Newsletter, this edition provides a specific focus on two SMP components: the Information Dissemination System (IDS) and the Attack Prediction modules.

This edition of the GAMMA Newsletter comes as preparations are made for the final GAMMA event which will be held in Rome on 15th November 2017. The event will be the opportunity to present the work and results achieved in GAMMA with a first-hand demonstration of developments carried out in the project during these years.

I therefore take the opportunity of this newsletter to invite users, stakeholders and security experts to the GAMMA final event. Please save the date and send your confirmation if you are interested to be on board!

by Giuliano d’Auria,
GAMMA Project Coordinator

GAMMA IN BRIEF

GRANT NUMBER:	312382
PROJECT COORDINATOR:	LEONARDO
CONTACT PERSON:	Giuliano d’Auria giuliano.dauria@leonardocompany.com
PROJECT WEBSITE:	www. gamma-project.eu
DURATION:	48 months (from 01/09/2013)
BUDGET:	14.8 € Million

SAVE THE DATE: GAMMA final event

“A new vision for ATM Security Management”

Next **15th November 2017**, GAMMA will organise in Rome (Italy) its final event “**A new vision for ATM Security Management**” providing the opportunity to witness first hand the results from one of the main R&D initiatives dealing with the management of Security within the ATM domain.

The vision of collaborative ATM security management is widely accepted as a principle guiding the implementation of an ATM Security Framework in Europe. GAMMA builds on these generally accepted principles and explores technological and operational options, implications and opportunities.

The GAMMA event is intended to add an R&D exploratory flavor to the discussions over the future shape of Security Management within the ATM domain.

The event will be centered on the concrete demonstration activities performed within the project, which will provide the starting point for a guided tour of the work done within GAMMA.

Save the date and contact **Giuliano d’Auria** (giuliano.dauria@leonardocompany.com) if you are willing to come on board!

The First Performance of the Integrated GAMMA Solution: The Full 3 Validation Exercise

Author: DLR

Introduction – Recap of the GAMMA Concept

After three years of intense work on the ATM security risk assessment, the security management framework, the ATM security functional and operational architecture, the development of GAMMA prototypes, as well as their stand-alone validation, the project achieved good progress and demonstrated its initial capabilities. In the first half of 2017, the project was ready for the next challenge: more complex threat scenarios involving different kinds of offences targeting different weak points in the ATM system.

In addition to directly defending affected systems against the interference, the overall idea is to exchange all security-relevant information with all persons and/or entities in charge, also involving civil-military cooperation. This significantly improves the overall awareness of any cyber attacks and the consequences, which enable to select countermeasures more appropriately, initiate coordinated countermeasures or activate preventive measures in advance.

The GAMMA solution has come up with a multi-level approach:

- ATM Security Management on Local Level: Security Management within an ATC unit, at an airport, at an aeronautical information management unit, at a unit of the weather service, within an airplane
- ATM Security Management on National Level: Information are collected and decisions are made for all units and stakeholders within a country
- ATM Security Management on European Level: Information are collected and decisions are made for all lower GAMMA levels within Europe

Six of seven prototypes developed within GAMMA are specific security systems designed for the local level: Information Exchange Gateway (IEG), Information Security System (ISS), Global Navigation Satellite System Security (GNSS), Secure ATC Communications (SACom), Satellite Communications Security (SATCOM) and Integrated Modular Communication Security (IMC) prototypes. All these systems work as detectors and collect information about ongoing attacks on systems where they have been installed. Some prototypes are even able to directly protect those installations and/or provide assistance to the user on local level in handling the incident.

The seventh prototype is the 'core' of the whole ATM security management solution of GAMMA: the so called Security Management Platform (SMP) which collects all security relevant information generated at the local level, builds up a complete security picture, detects coherencies by correlation algorithms and provides assistance in decision making for the operator who is responsible for initiating possible countermeasures. Information can be disseminated to the local level, to the higher European level or even to military authorities if deemed necessary. At this point, the GAMMA concept foresees a new role, the so called 'GAMMA operator'. This person is specialized on ATM security crisis management and well trained on relevant regulations, procedures and on technical systems playing a role in ATM.

The Threat – Coordinated and Uncoordinated Attacks

On September 11th, 2001 the world was confronted with a completely new dimension of terrorist attacks. This obviously coordinated attack was possible because of a lack of information exchange and situational awareness between security management entities although the whole attack lasted a relatively long time of more than one hour.

To be able to systematically categorize and identify coordinated attacks a clear definition is needed. For the further work in GAMMA, the following definition was found and served as a guideline:

A coordinated attack scenario is an attack, in which:

- The single attacks are of negligible effect when performed standalone due to missing synergy effects from the other single attack (e.g. distraction, overload, amplification etc.)

And/or

- The single attacks must be aimed at exactly the same target at nearly the same time.

And/or

- The single attacks must be of a similar kind and must be aimed at roughly the same sort of targets at nearly the same time.

The term 'nearly the same time' unfortunately is not that precise. Therefore, it can be further assumed that attacks happen at 'nearly the same time' when the time frames of visible effects and aftereffects overlap. This means for example if an attack takes place at timestamp T=0 and the effects and aftereffects extend up to timestamp T=20, another attack taking place at timestamp T=45 would be considered as isolated and not as happening at 'nearly the same time'.

The coordinated 9/11 attack would be a mixture of bullet point 2 and 3 above according to this definition. Two airplanes hit the World Trade Centre (WTC) in New York City, which are two single acts hitting the same target. The attack focused at the Pentagon in Washington DC used the same method: using a hijacked airplane as a weapon to cause serious damage to a building of public interest. The time frames of visible effects and aftereffects were about several days and clearly overlapped.

Within the integrated validation exercises in GAMMA different attack scenarios with a similar level of complexity were used while also several independent, uncoordinated attacks were simulated. In the Fully Integrated Validation Exercise III (or short: Full 3), a coordinated cyber-security attack on aeronautical weather information services was simulated. The goal of this coordinated attack was to manipulate safety-relevant meteorological data (namely the measured air pressure, which is essential for altimeter settings) at two different European airports in two different countries within a time interval of a few minutes. If not detected, this false information could likely cause the risk of controlled flights into terrain (CFIT), which is a well-known type of accident with a number of examples in aviation history. In parallel, an uncoordinated hacking attack to on-board communication systems from inside of an airplane was simulated.

Combating the Threats/Attacks

On local level, two prototypes have been developed to counteract these threats:

The IEG (Information Exchange Gateway) prototype was built by Airbus CyberSecurity to protect web services from XML-based threats like the injection of spurious weather information or different kind of attacks against the SWIM (System-wide Information Management). This prototype aims at enhancing the traditional detection approach by providing mechanisms capable of detecting offensive contents and intercepting them by applying advanced data packet inspection methods in which malicious packets are directly blocked and alerts are instantly sent to the SMP.

The second prototype on local level is the IMC prototype, which is designed to secure integrated communication networks and systems on board of an airplane and was developed by Thales UK. This prototype offers functionalities to handle on/off board application attacks, insertion of subverted software, and directly block unauthorized access to the IMC and then send report to the SMP if required.

Although the direct defense of these parts of the attack scenario was successfully accomplished on local level, there is still no awareness about the magnitude, the potential and the coordinated nature of the attempts to manipulate the aeronautical weather data. This lack of awareness is very dangerous because it could well be that the coordinated attack is still ongoing and could at some time hit an unprotected system at another airport, maybe in another country. Therefore security-relevant information is shared between the different levels of the GAMMA solution (see Figure 1). The IEG prototypes that defended the attempts send automatic reports to the national level SMP of the corresponding countries. As long as there is just one airport affected by the attack in this country, there is no possibility to already apply correlation algorithms. But as SWIM is a European-wide service, an attack on meteorological data exchanged via SWIM could be of relevance for the European level. Therefore, the

GAMMA operators at national level forwards sanitized information about the attack happening in their country to the European level according to defined rules. On European level the coordinated nature of the attack is immediately detected by correlation algorithms. Several countermeasures can now be triggered, such as a general warning is distributed directly to the user via SWIM or a specific warning is sent back to national levels; either to the SMP in a third country which is not yet hit by the attack or as feedback to an already affected country giving notification that this attack is coordinated and of a bigger magnitude.

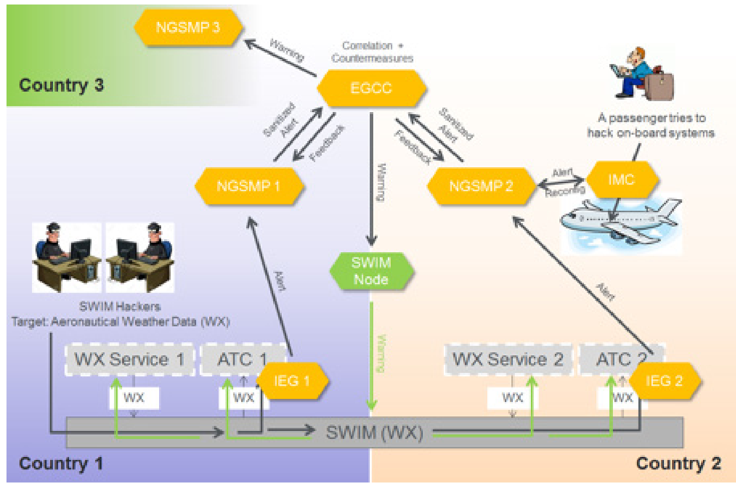


Figure 1: Attack and Response Scenario of the Full 3 Exercise

For the Full 3 exercise this scenario was successfully simulated by using a fully connected geo-distributed setup involving prototypes or system components owned by Leonardo, Airbus CyberSecurity, Thales UK, 42Solutions and Boeing Research and Technology Europe. These prototypes or system components were located in Chieti (Italy), Elancourt (France), Reading (UK), Eindhoven (Netherlands) and Madrid (Spain). Security Management Experts from the ATM domain took the role of the GAMMA operators in the final runs. The whole exercise was led by DLR using a multi-screen working position located in Braunschweig (Germany). A group of external observers from different ANSPs monitored the exercise from this position, a second group observed the exercise side-by-side with the GAMMA operators in Chieti (Italy).

The final runs of the Full 3 exercise took place on 4th May 2017 and were connected to a workshop with the mentioned experts at each site.

Figure 2: Multi-Screen Working Position in Braunschweig during the Final Run of the Full 3 exercise

Lessons learned

Important outcomes of the Full III exercise were empirical data about reaction times of the GAMMA operators, transmission time of security relevant information in this geo-distributed setup and duration until the coordinated nature of the attack was identified. Additionally, it was examined if and how false alarms or missing information occur in the solution designed by GAMMA and the implications for Security Management.

In addition, valuable feedback was collected from external ATM security experts either participated as observers or as GAMMA operators, providing insights into upcoming challenges before implementing the GAMMA solution into the real world as well as benefits of the GAMMA solution provides to the ATM community as a whole; and specifically regarding ATM security improvements.

ARTICLES

Information Dissemination System

Author: 42 Solutions

I.INTRODUCTION

The GAMMA vision is to adopt a holistic approach to assess ATM security, in line with SESAR. GAMMA objectives are to:

- Develop a Global ATM Security Management framework, representing a concrete proposal for the day-to-day operation of ATM Security and the management of crises at European level.
- Define the architecture of an ATM security solution, suitable to support the security management of the global ATM system.
- Design and implement prototype components of the GAMMA solution so as to demonstrate the functionalities and operations proposed for the future European ATM.
- Set up a realistic validation environment, representative of the target ATM solution, through which to perform validation exercises aimed at validating the feasibility and assessing the adequateness of the procedures, technologies, and human resources issues proposed.

II. THE CONTEXT

ATC currently relies mainly on verbal communication in crisis situations between stakeholders. One of the approaches within GAMMA is to continuously share security information among the different ATM actors, providing overall situational awareness of the security status of the ATM as a whole, as well as a basis for identifying threats through extended correlations of isolated incidents.

As part of the work performed in GAMMA the following improvements were identified in the area of verbal communication during crisis situation:

- Improvement IMP-DL-REPORT: Exchange of ATM incident-related information between civil and military via data link
- Improvement IMP-STD-REPORT: Harmonisation of information standards and reporting procedures about incidents

III. THE CONCEPT OF OPERATIONS

The GAMMA Concept (see Figure 1) has been defined having in mind principles and concepts related to Security Management in a collaborative multi stakeholder environment.

The GAMMA proposed solution contains a network of distributed nodes (see Figure 2). Each node is embedded within the ATM system and is providing interfaces to (ATM) internal and external security stakeholders. The Information Dissemination System is a module of the Security Management Platform prototype (SMP), enabling the dissemination of security information through the multilevel architecture as proposed by the GAMMA solution.

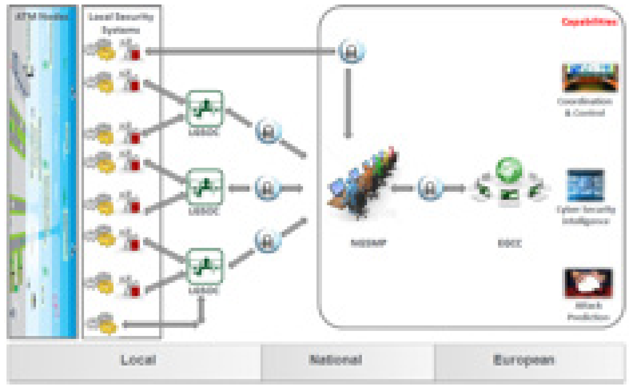


Figure 1: The GAMMA Concept

IV. INFORMATION DISSEMINATION SYSTEM CONCEPT

The Information Dissemination System (IDS) is an open architecture platform and can interact with a multitude of event sources. In the scope of GAMMA it receives security information from other modules within the Security Management Platform (SMP) over an Event Bus (using the open messaging system product Kafka from the Apache Software Foundation). The information is retained within the IDS and can be accessed by the user.

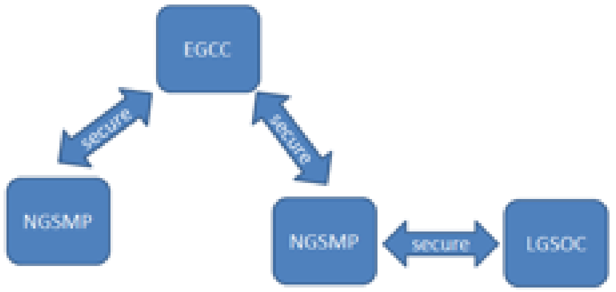


Figure 2: Gamma network of distributed nodes

The IDS platform facilitates the secure cross-SMP information dissemination. Each IDS instance connects to one or more other SMP. IDS nodes form a network (see Figure 2) between SMP's to share the security information.

All received security information within IDS will be disseminated to one or more involved stakeholders (at local, national, military and/or European level) on a need-to-know bases by applying dissemination rules on the content of the security information, the source and the expected destination.

After applying the dissemination rules on the security information the designated SMP nodes are known and the encrypted security information will be sent to these designated nodes.

These SMP nodes receive, store and forward the security information via their Event Bus to the other modules within their SMP node domain.

Other than disseminating security information between nodes coming from other SMP modules, the Information Dissemination System provides situational awareness - in both the temporal and positional domains - of (potential) incident related information (e.g. alarms, security intelligence information) received from connected detection systems. It is based upon the views presented to Air Traffic Control Association (ATCA) in the scope of Civil-Military Cooperation [1].

The IDS provides the means to embellish the situational display with dynamic information (e.g. traffic, weather, etc.) from external systems.

Within GAMMA, IDS demonstrates the inclusion of the air traffic picture based on ATM data coming from external track and flight data sources. The situational awareness display provides several maps to support concise situational awareness fitting the corresponding level of detail to support and expedite incident response management.

V. ARCHITECTURE OF IDS

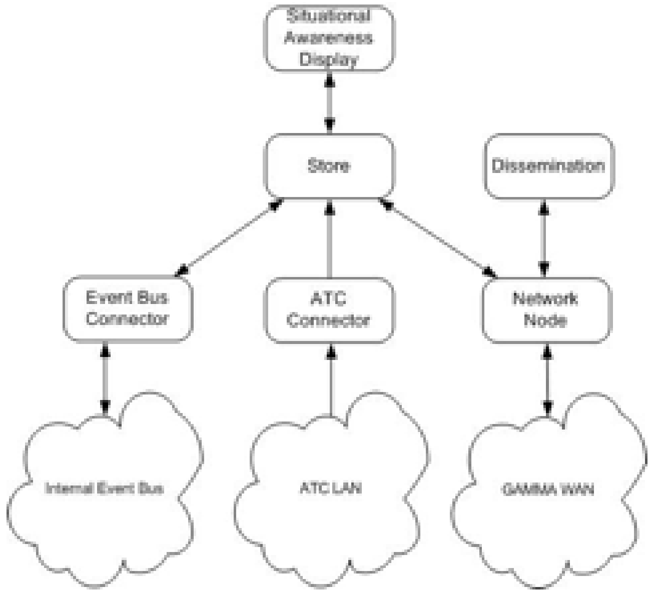


Figure 3: IDS components

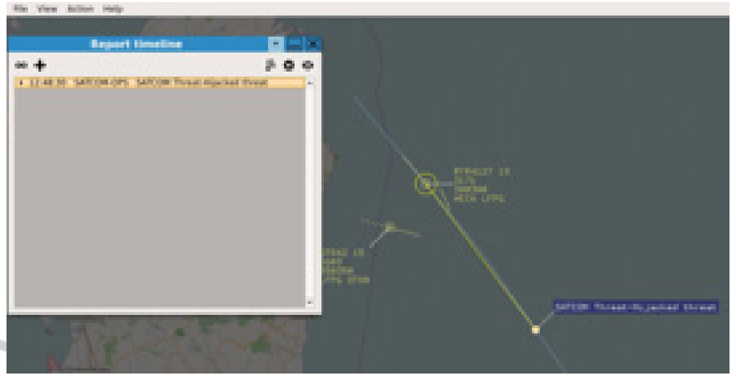
The IDS architecture consists of the following components (see Figure 3):

- The Event Bus Connector component interfaces with the other SMP modules responsible for the XML decoding / encoding of incoming/outgoing reports and requests/responses.
- The Store component stores all reports and ATM data (tracks and flight plans) received by IDS, correlates reports with other reports and ATM data. It forwards disseminated reports to the Event Bus Connector component and/or the Network Node component for dissemination to the other SMP modules.
- The Situational Awareness Display component displays the reports and ATM data on temporal and positional domains.
- The Dissemination component contains the dissemination rules for connected SMP nodes within the GAMMA WAN and determines based on the dissemination rules whether the reports are granted for one or more of the SMP node(s).
- The Network Node component disseminates the reports to the target connected SMP nodes.
- The ATC Connector component is the interface with ATC network.

VI. VALIDATION ACTIVITIES

The overall objective of the validation work package of the GAMMA project is to validate the GAMMA Security Management concepts, together with their related operational scenarios, procedures and developed technologies. The IDS module as part of the GAMMA Security Management is validated within partial integration 1(PI1) and full integration 3 (FI3) validation exercise.

The partial integration1 validation scenario shows a hijack and an attack on the on-board SATCOM equipment of the aircraft and a close coordination via voice and via datalink between civil and military authorities. The attack on the on-board SATCOM triggers an alarm on the last known position on national level and based on this information the national authorities decide to disseminate the alarm to the military authority using IDS (see Figure 4).



SATCOM Threat-Hijacked threat

Figure 4: IDS in PI1 validation exercise

The full integration 3 validation scenario (see Figure 5) shows coordinated and uncoordinated attacks (SOAP/https security attacks on SWIM, on-board attacks on the aircraft systems) in 2 countries. At European level it is decided to inform a third country about these attacks using IDS.

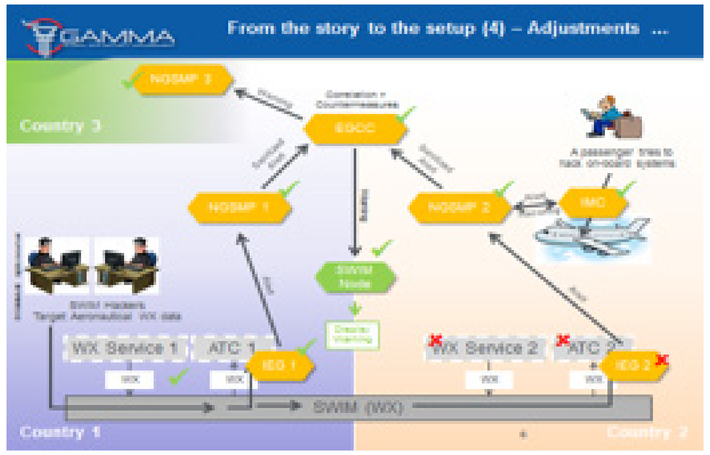

GAMMA
From the story to the setup (4) – Adjustments ...
NGSMP 3
Country 3
Correlation + Countermeasures
EGCC
A passenger tries to hack on-board systems
NGSMP 1
NGSMP 2
IMC
SWIM Node
SWIM Hackers
Target Aeronautical WX data
WX Service 1
ATC 1
IED 1
WX Service 2
ATC 2
IED 2
WX
SWIM (WX)
Country 1
Country 2

Figure 5: FI3 validation scenario

VII. CONCLUSIONS

Within GAMMA a basis for standards has been laid down for information sharing, but a harmonised information standard is not yet defined and will represent a challenge for a follow up project. .

REFERENCES

[1] National Security, When Time is of the Essence, Strijland W, 42 Solutions, ATCA Conference Proceedings, Winter 2014: www.atca.org/2014-Conference-Proceedings

ATTACK PREDICTION MODEL FOR FUTURE ATM SYSTEMS

Authors: D.Kolev and G.Markarian - Lancaster University, UK

Current **practices and standards for security risk management** involve the identification of **security risks** and the **implementation of associated controls** at a system- or component-level. The risk assessment is typically performed by experts and based on a mix of qualitative and quantitative methods. However, the higher levels of interconnectivity across infrastructure components require the **analysis of threat propagation within and across the associated supply chains**. There exists a wide variety of security risk management methodologies, but few are specifically tailored to the design and development process and to the best of our knowledge, no reliable methodology is available yet for risk management on services involving complex infrastructures such as the health system.

Given the high amount of variables and interdependencies involved, it is essential to employ analytics to assist the process of risk management and evaluation in ATM systems and infrastructures. Deployment procedures include installations (both public and private that need appropriate security levels), that are planned beforehand, in parallel with the development process. That kind of procedures are often projected using an applied mathematics approach for security, usually derived from the domain of probabilistic models and multi-agent models.

Probabilistic modelling is used in order to capture the uncertainty of the observed data, which may be caused by unpredictable factors or by the model inaccuracy, in parallel with the general dependency of the observed factors. Such systems may be employed for security/safety objectives to infer the "hidden" global values, that describe the general state of the ATM system, for instance different failure conditions. **Multi-agent models** are especially relevant for the systems that are used for behavior modelling, recommendation, and decision support.

One of the deliverables of the GAMMA project is a novel attack prediction model specifically developed and optimized for future ATM systems. The developed **Attack Effect Prediction Module (AEPM)** is designed using both of the methodologies, where **Probabilistic Bayesian inference** is used for current state estimation and **Game Theory** is used to perform the prediction based on the estimated characteristics of the adversary. The protected ATM infrastructure is modelled using graph-based approach, that is similar to the Attack Trees method and Network Security Games, that encodes the main steps required to perform an attack. The developed model may be considered as a synthesis of the attack scenarios, defined for the protected system and throughout the GAMMA project numerous predefined security threats were analysed and simulated. This allows the graph instantiation procedures to be interlinked with the standard SecRAM methodology, which ensures an expert basis for the model. The designed graph links the mathematical formalism and the main definitions used in risk analysis, i.e. Supporting and Primary Assets, Attack scenario, etc.

The design AEPM supports two modes:
(i) dynamic for real-time risk prediction;
(ii) off-line for security audits of ATM systems.

In dynamic mode, AEPM obtains and processes the information received from diverse sensors, placed within the protected system, which are considered as event detectors. It is important to mention that within the scope of the GAMMA project, the AEPM may process the information from systems of different levels of perception (like cyber intrusion detection for high perception or incorrect login attempt for low), serving as Data Fusion engine. This engine can correlate alarms and detections from different heterogeneous sources (idea, similar to bagging from Data Mining). The AEPM uses the received information to estimate the security status of the system ("under attack" flag probability) and characteristics of the adversary, such as abstract "skill" level and possible intention of the adversary. Based on the estimated information and the structure of the graph that describes the system, a prediction of possible actions of the attacker may be inferred.

In off-line mode, the model is applied to a predefined graph corresponding to a given ATM infrastructure and evaluates its security resilience level. The model can be used for optimsing security resilience by recommending optimal locations of even detectors and providing the desired cost/benefit ratio.

Figure 1 bellow illustrates one of the developed graphs emulating ATM computer network infrastructure. In this particular architecture two possible entries for the attacker (top of the graph) and a number of security assets (bottom of the graph) are defined. All the possible paths from an entry to a security asset are monitored by event detectors and the system calculates the instant probability of an attack.

As it follows from this figure, the developed model provides real time probability of an attack from all current users of the infrastructure. In addition, the initial problem statement may be significantly explored, by enhancing the structure and the space of the adversary's skill variable, incorporating the dependency model between different event detectors.

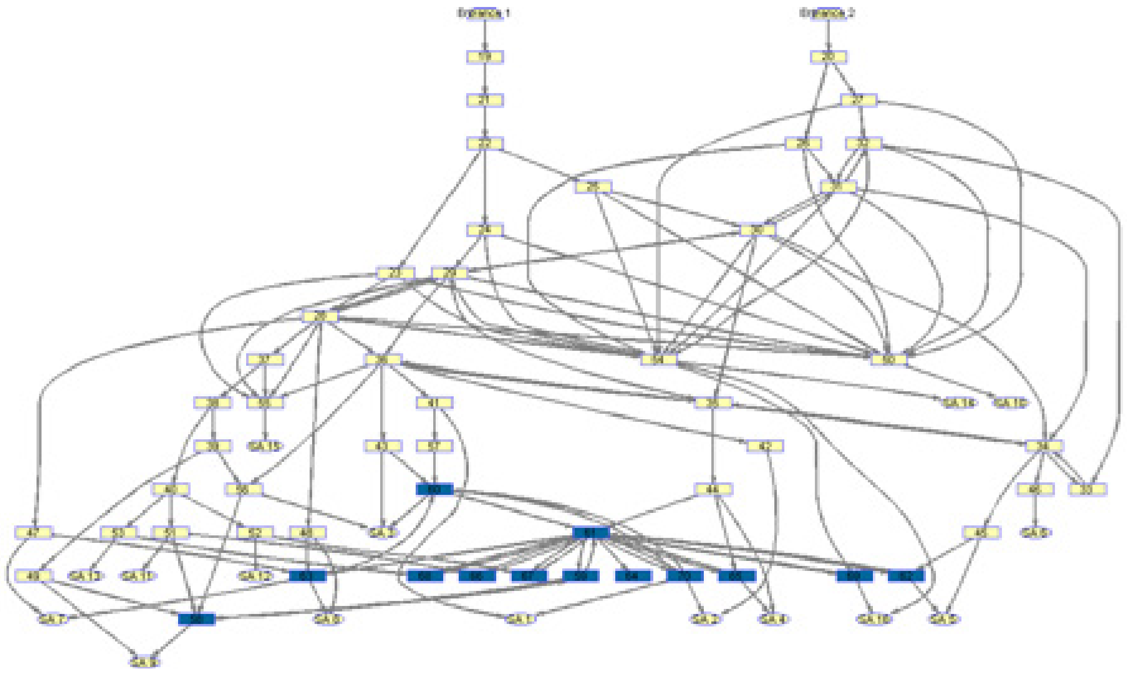


Figure 1: Graph model mapping interdependencies and potential outcomes

DISSEMINATION

NEWS

GAMMA Workshop in Rome

On 6th July 2017 a workshop was organized in Rome, following the completion of the latest integrated validation exercise aimed at demonstrating how GAMMA handles uncoordinated attacks within the same country.

The exercise scenario involved a hijacking event in which the SATCOM communication was deliberately disconnected in an area out of civil radar coverage, while satellite navigation was jammed in a separate unconnected incident. The scenario also included new civil military cooperation principles and innovative ideas aimed at complementing the surveillance information displayed to the controller with contributions sent by the military. The exercise held on 23rd June was implemented by setting up a distributed platform interconnecting prototypes and validation assets (including deployed real assets) developed by Airbus DS, Leonardo, Thales Avionics, Thales Alenia Space and 42 Solutions, while DLR provided the overall view of the exercise and was observed by a representative of French Air Force.

The workshop was attended by experts and stakeholders mainly representing the military domain, in view of the significance of the scenario for civil military coordination.

Stakeholders and experts involved in the exercise and in the workshop recognized that the GAMMA concept implemented in the scenario enables an early reaction by the military to hijacking events, saving valuable time for activating the scrambling of fighters.

GAMMA Validation Trials to Detect Coordinated Attack on National Level

On May 15th and 16th 2017, five runs were performed to validate the detection of a coordinated attack on national level. Three GAMMA security prototypes acted in the geo-distributed simulation: The ISS (Information Security System) in Florence (premises of Leonardo), the SMP (Security Management Platform) in Chieti (at Leonardo premises) and SACom (Secure ATC Communication) in Braunschweig (at the German Aerospace Center, DLR premises). The trials were executed as human-in-the-loop simulations supported by 6 test persons: four ATCOs in Braunschweig (in Germany) and two Leonardo colleagues in Chieti (Italy).

FUNDING OPPORTUNITIES

SMEInst-10-2016-2017: Small business innovation research for Transport and Smart Cities Mobility

Deadlines Phase 1 in 2017: 7 November 2017
Deadlines Phase 2 in 2017: 18 October 2017

The SME instrument addresses the financing needs of internationally oriented SMEs, in implementing high-risk and high-potential innovation ideas. It aims at supporting projects with a European dimension that lead to major changes in how business (product, processes, services, marketing etc.) is done. Actions to develop new services, products, processes, technologies, systems and combinations thereof that contribute to achieving the European transport and mobility goals defined in the 2011 Transport White Paper could be particularly suited for this call.

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/smeinst-10-2016-2017.html

2017 SESAR JU Young Scientist Award 2017

Deadline: 1 October 2017

The SESAR Young Scientist Award, aims to recognise young scientists with high potential contributing to any SESAR activity by supporting the scientific development of “Air Traffic Management and Enabling Technologies”. Candidates must be a Young Scientist who has contributed to scientific achievements within a Bachelor or Master Thesis (which must have been completed not more than 2 years ago) or part of an on-going PhD, and who are resident of an EU Member State or an Associated Country to the Horizon2020 Research and Development Framework Programme (H2020). The Young Scientist applying must be able to show scientific achievement that is clearly relevant to the Single European Sky (SES) and in particular SESAR, covering ATM, related Airport and Air Vehicle areas of research.

https://www.sesarju.eu/news/applications-open-sesar-ju-young-scientist-award-2017

ERC Synergy Grant

Deadline: 14 November 2017

ERC Synergy Grants are intended to enable minimum two to maximum four Principal Investigators and their teams to bring together complementary skills, knowledge, and resources in new ways, in order to jointly address ambitious research problems. The ERC's frontier research grants operate on a 'bottom-up' basis without predetermined priorities. The aim is to promote substantial advances at the frontiers of knowledge, to cross-fertilize scientific fields, and to encourage new productive lines of enquiry and new methods and techniques, including unconventional approaches and investigations at the interface between established disciplines.

http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/erc-2018-syg.html

For more information about funding opportunities please contact c.salas@ciaotech.com.

CONSORTIUM

LEONARDO
WWW.LEONARDOCOMPANY.COM

Airbus SAS
WWW.AIRBUS.COM

Boeing
WWW.BOEING.COM

Airbus Defence and Space
WWW.AIRBUSDEFENCEANDSPACE.COM

Airbus Defence and Space Cybersecurity
WWW.CYBERSECURITY-AIRBUSDS.COM

CiaoTech
WWW.CIAOTECH.COM

DLR
WWW.DLR.DE/FL/

Airbus Group Innovations
WWW.AIRBUSGROUP.COM

ENAV
WWW.ENAV.IT

Isdefe
WWW.ISDEFE.ES

Lancaster University
WWW.LANCASTER.AC.UK

RNC Avionics
WWW.RNC-AVIONICS.COM

Romatsa
WWW.ROMATSA.RO

SEA
WWW.SEAMILANO.EU

Thales Alenia Space
WWW.THALESALENIASPACE..COM

Thales Avionics
WWW.THALESGROUP.COM

Thales UK Limited
WWW.THALESGROUP.COM/UK

Ústav Informatiky
UI.SAV.SK

42 Solutions
WWW.42SOLUTIONS.NL

ACKNOWLEDGEMENT

The GAMMA Project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under Grant Agreement Nº 312382.