A New Vision for ATM Security Management

The Security Management Platform

Claudio Porretti
Security and Information Systems
FINMECCANICA S.p.A.
Rome, Italy
claudio.porretti@finmeccanica.com

Denis Kolev
University of Lancaster
Lancaster, UK
denis.g.kolev@gmail.com

Raoul Lahaije
42Solutions
Eindhoven, The Netherlands
raoul.lahaije@42solutions.nl

***Abstract*—**

*The aim of this paper is to describe a new vision for ATM Security Management that is proposed by the GAMMA project, and implemented by its "core" prototype called **Security Management Platform**.*

GAMMA is an FP7 project with the goal of developing solutions capable to manage emerging ATM vulnerabilities. The GAMMA vision recognises the opportunities opened by a collaborative framework for managing security, building a solution based on the self-protection and resilience of the ATM system, with the possibility to share security information in a distributed federated environment.

This concept is implemented with the Security Management Platform prototype, and can be conceptualized as a network of distributed nodes embedded within the ATM system, providing interfaces to (ATM) internal and external security stakeholders.

The Security Management Platform prototype provides a basis for the management of security throughout phases, from prevention to the identification of security incidents and the efficient resolution of the resulting ATM crises.

Keywords *– ATM, Security Management, Vulnerabilities, Collaborative Framework, Security Information Sharing.*

I. Introduction

The GAMMA vision is to adopt a holistic approach for assessing ATM security, maintaining alignment with SESAR and reaching the following main objectives:

- Extend the scope of threat assessment performed within SESAR to a more comprehensive system of systems level, inclusive of all ATM assets and all forms of threats.
- 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

The new ATM system must take into account the changes in security risk profiles, due to cyber attacks, telecommunication systems spoofing and ground physical attacks, that according to the new ATM architecture can spread their negative effects from one node to a global level, due to chain reactions and domino effects.

This situation calls for a holistic vision of ATM security, as pursued by GAMMA, to ensure:

- Continuous sharing of 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;
- Means for supporting the resolution of the security crises, minimizing disruptions and repercussions to the system as a whole
- Improved capabilities (operational and technological) to face emerging threats.

III. The Concept of Operations

The GAMMA Concept has been defined having in mind principles and concepts related to Security Management in a collaborative multi stakeholder environment

The GAMMA solution can be conceptualised as a network of distributed nodes embedded within the ATM system and providing interfaces to (ATM) internal and external security stakeholders.

GAMMA establishes three different levels for managing security:

- the European level represented by the European GAMMA Coordination Centre (EGCC),
- the National level represented by the National GAMMA Security Management Platform (NGSMP)
- the Local level represented by local security systems as well as Local GAMMA Security Operation Centers (LGSOC).

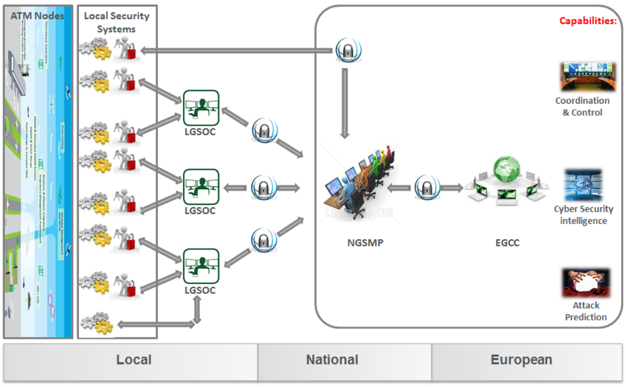


Figure 1. The GAMMA Concept.

The most important concept of the GAMMA project is the sharing of security information such as security alerts, possible countermeasures, security reports, between ATM stakeholders.

The sensitive information, generated at local and national level, that has to be disseminated to the European level, can be (if necessary) opportunely modified so as to eliminate sensitive aspects.

IV. The Security Management Platform

The federated architecture concept mentioned above is implemented by the Security Management Platform (SMP) prototype.

The SMP is intended to provide Situational Awareness (applying cross-correlation techniques of events) and Decision Support functionalities, supporting the coordinated management of ATM security.

For this purpose the shared platform includes specific capabilities such as Cyber Security Intelligence and Attack Effect Prediction, in order to provide decision support to GAMMA operators, that are the stakeholders interfacing the SMP system, with the aim of managing ATM security.

Moreover, the SMP includes an Information Dissemination System that allows the dissemination of security information through the multilevel architecture proposed by the GAMMA solution.

A. Architecture

The SMP subsystems are connected through an enterprise application bus (Internal Event Bus) that enables the cooperation among different modules.

Another application bus (External Event Bus) is used to connect the national level SMP to the European level SMP and to local security systems such as LGSOCs and other security prototypes.

Each subsystem has its own visualization module (HMI) that is included in the Visualization Module of the Command and Control subsystem.

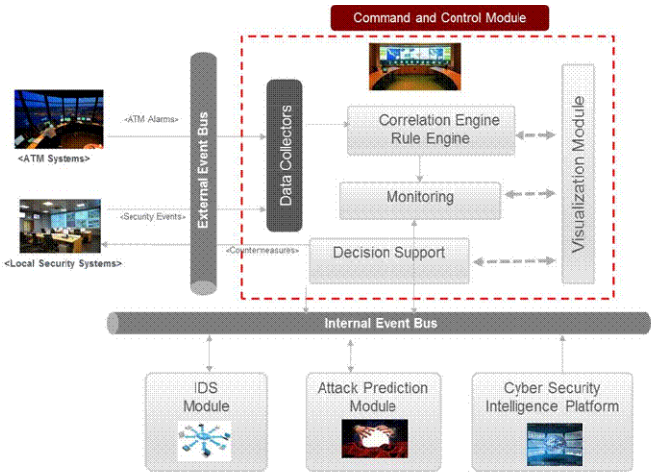


Figure 2. SMP architectural lay-out.

SMP receives input from:

- Local Security Systems (LGSOC or other Prototypes) (security events / detections)
- ATC systems (alerts from systems within the ATM domain)
- Other SMPs (disseminated alerts / messages)
- The internet (open source information about possible attacks in social networks, chats, etc.)

SMP outputs are:

- Security reports (to Local Security Systems or to other SMP)
- Correlated alarms due to the correlation function
- Recommended Countermeasures (to Local Security Systems or to other SMP)
- Attack effect prediction reports (to Local Security Systems or to other SMPs)
- Alarm clearing (to some other Prototypes)

The following paragraphs describe the Security Management Platform main functions

B. *Command and Control subsystem*

This subsystem provides Alarm Correlation, Security Monitoring and Decision Support for Incident/Crisis Management.

It includes a Data Collector for gathering security events from Local Security Systems and ATC systems, correlating them using a Correlation Engine and displaying the resulting alarms to the operator with the Monitoring facility.

A decision support function allows the operator to provide possible countermeasures to Local Security Systems or other SMPs.

A sanitization function is also available in order to opportunely modify sensitive information before transferring them to the IDS module for dissemination.

C. *Cyber Security Intelligence Platform*

The Cyber Security Intelligence Platform (CSIP) is based on an open source intelligence service provided in cloud by Finmeccanica. The intelligence module is connected to the Command and Control module by API connection .

CSIP provides GAMMA operators the possibility to obtain relevant information about possible (cyber) attacks on ATM systems, crawling the internet though open sources such as social networks, in order to determine the sentiment and/or threats related to a particular target. They also allow to identify the motivation, the characteristics and the identities of the attackers.

The main functions of CSIP are listed below:

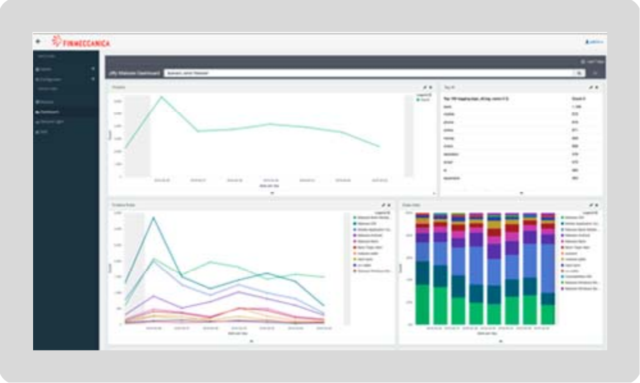
- Intelligence Scenario Configuration
- Crawling of RSS, Twitter, Facebook, PAD
- Indexing & Searching
- Sentiment analysis
- API for Security Reports exportation
- e-mail alerting possibility

The tools available for the operator are:

- Searching semantic search of information system impairments, such as cyber attacks and data breach
- Dashboards: customized dashboard to provide aggregate views according the specific analyst needs
- Case Manager: visual analysis of complex situations
- Reporting: automatic report generation related to either corporate data subtraction or any detected attack under preparation (pre-planned attack)

Having defined a scenario of interest described by the specification of patterns, keywords and a time interval, the GAMMA operator using an advanced mechanism of crawling and analysis, can acquire data from monitored sources, identify patterns related to the particular scenario and extract generic or specific entities. The processing of the data found in this way allows then to obtain meta-data information, which will be subsequently used for analysis.

The results of investigations conducted are immediately usable by analysts through the dedicated dashboard.



.

Figure 3. CSIP dashboard.

Once relevant information is obtained, the GAMMA operator can produce a Security Report that can be sent to connected ATM domains and disseminated (through the IDS module) to other SMPs at national or European level.

D. *Attack Effect Prediction Module*

As was stated before, the SMP serves as a central collector and analyzer of the information generated by diverse set of security controls and event detectors. In this case the joint and sequential analysis of the received information may serve a crucial task, as the Data Fusion enabled by the SMP may reduce the number of false alerts [6] and enable temporal analysis of the actions of the adversary.

The Attack Effect Prediction (AEP) Module is a decision support SMP sub-system that provides a joint assessment of the information received from different sensors (event detectors) represented at the system.

Received information is used to address the following problems:

- Is the system under attack?
- What is the qualification/skill of the adversary?
- What are the targets selected by the adversary?

In order to resolve the stated problems, the overall system should be formally described.

As a system descriptor a directed graph structure is used, following the approach used in Network Security Games (NSG) [7].

The graph encodes all Supporting Assets (SA) as a subset of nodes and all threat scenarios as a set of paths to the SAs, that form the graph.

Additionally, an impact value for each type of attack for each security control is given (or a set of values for different Impact Areas).

Security controls and event detectors are linked to the nodes of the graph.

The model assumption is that the adversary selects a subset of paths to the SAs and security controls and event detectors may mitigate the impact values or detect the attacker's actions.

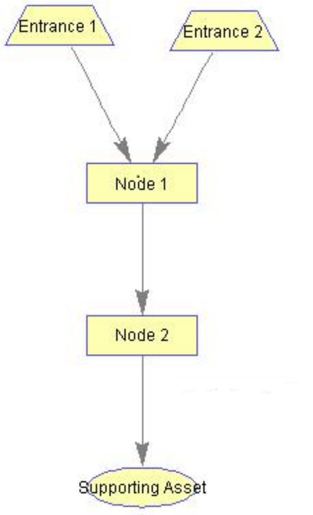


Figure 4. Example of the graph model.

Using the proposed graph model formalization, the *state* of the adversary may be described as a tuple (P,S,T). P stands for the position (node in the graph), which may be *empty* in case of no attack taking place. S is the skill-vector of the adversary, which describes the ability to overcome the security controls. T stands for the targeted SA by the attacker.

Thus, the system estimates the state of the adversary for each moment of time given the received event detections.

Parameters P,S of the adversary's state are estimated using Dynamic Bayesian Network for sequential data analysis, which is similar to the approaches used for Bayesian Multiple Target Tracking [8].

The AEP system updates its' internal parameters using newly received information for each moment of time, similar to the correction step of Bayesian Filters, updating the adversary's state beliefs (probability distribution). Parameter T is estimated based on game theory methods.

From the estimated probability distribution over adversary's state a subset of most probable states are selected.

An expected impact is estimated for each of the selected states, based on the predefined impact values, estimated adversary's skills and implemented security controls' properties. Derived information is reported to the overall system via the Event Bus

E. *Information Dissemination (sub)System*

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 SMP over an Event Bus (using the open messaging system product Kafka from the Apache Software Foundation [5]). The information is retained within the IDS and can be accessed by the user.

IDS facilitates manual as well as automatic dissemination of security information to other stakeholders at national or European level.

Each IDS instance of SMPs at national level is connected to the IDS instance of the SMP at European level. When IDS instances are up and running, a network (see Figure 5) is built up between SMP's to share the security information.

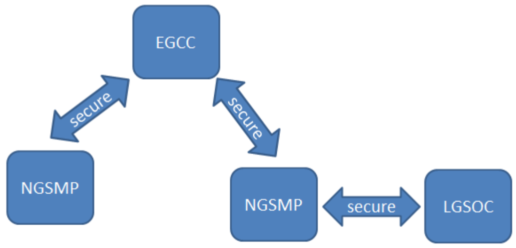


Figure 5. Network of SMP nodes.

All the received security information within IDS will be disseminated to one or more involved stakeholders (at local, national and/or European level) on an 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.

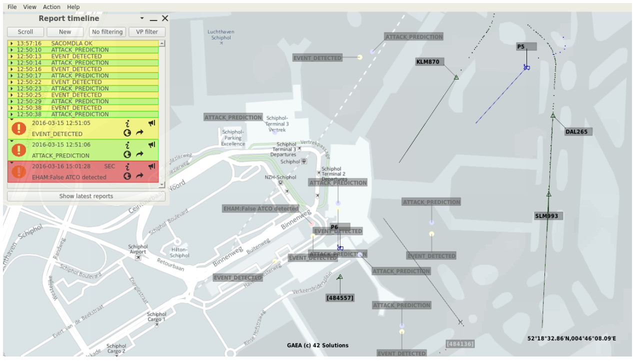
These SMP nodes receive, store and forward the security information via their Event Bus to the other modules within their SMP node domain.

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 information, intelligence information) received from connected detection systems.

It is based upon the views presented to ATCA in the scope of Civil-Military Cooperation [4]**.**

The information is presented on a concise situational awareness display (see Figure 6) with the possibility to zoom to the infrastructure level or system level.

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



File View Action Help

Report timeline

Scroll | New | No filtering | VP filter

13:57:16 SACOMDLA OK
12:50:10 ATTACK_PREDICTION
12:50:13 EVENT_DETECTED
12:50:14 ATTACK_PREDICTION
12:50:16 EVENT_DETECTED
12:50:17 ATTACK_PREDICTION
12:50:22 EVENT_DETECTED
12:50:23 ATTACK_PREDICTION
12:50:25 EVENT_DETECTED
12:50:29 ATTACK_PREDICTION
12:50:38 EVENT_DETECTED
12:50:38 ATTACK_PREDICTION

2016-03-15 12:51:05
EVENT_DETECTED

2016-03-15 12:51:06
ATTACK_PREDICTION

2016-03-16 15:01:28 SEC
EHAM:False ATCO detected

Show latest reports

Figure 6. IDS Situational Awareness Display.

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.

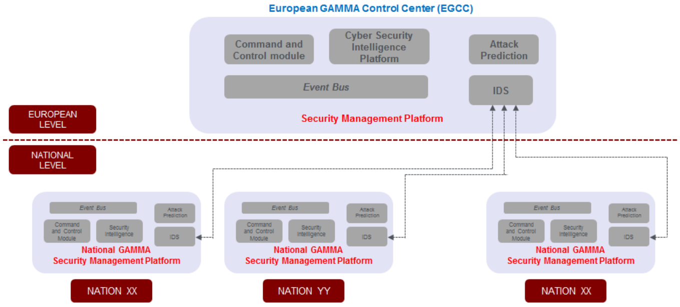
V. Multilevel Implementation

As mentioned above GAMMA establishes three different levels for managing security:

- the European level represented by the European GAMMA Coordination Centre (EGCC),
- the National level represented by the National GAMMA Security Management Platform (NGSMP)
- the local level represented by local security systems, namely "Local GAMMA Security Operation Centers" (LGSOC).

In terms of instantiations of the SMP this kind of approach foresees:

- one SMP instance in the EGCC
- one SMP instance for each NGSMP



European GAMMA Control Center (EGCC)
Command and Control module
Cyber Security Intelligence Platform
Attack Prediction
Event Bus
IDS
Security Management Platform
EUROPEAN LEVEL
NATIONAL LEVEL
Event Bus
Attack Prediction
Command and Control Module
Security Intelligence
IDS
National GAMMA Security Management Platform
NATION XX
NATION YY
NATION XX

Figure 7. The SMP implmentation in the multilayer approach.

The SMPs at national level are connected to the SMP at European level through the IDS modules.

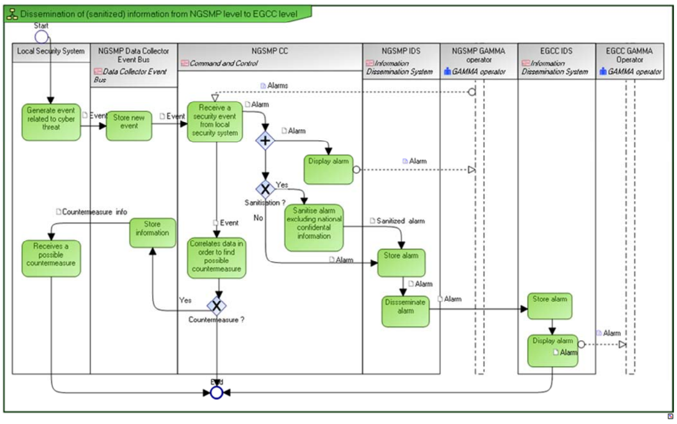
Each SMP at national level is connected to national Local Security Systems and ATM systems.

VI. A Validation Scenario

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.

An example of the various scenarios that have been prepared for validation purposes is the one illustrated in figure 8.

This scenario is related to the dissemination of (sanitized) information from NGSMP level to EGCC level, providing possible countermeasures to Local Security System about an ongoing attack.



Dissemination of (sanitized) information from NGSMP level to EGCC level
Start
Local Security System
NGSMP Data Collector Event Bus
Data Collector Event Bus
NGSMP CC
Command and Control
NGSMP IDS
Information Dissemination System
NGSMP GAMMA operator
GAMMA operator
EGCC IDS
Information Dissemination System
EGCC GAMMA Operator
GAMMA operator
Alarms
Generate event related to cyber threat
Event
Store new event
Event
Receive a security event from local security system
Alarm
Alarm
Display alarm
Alarm
Yes
Sanitisation ?
No
Sanitise alarm excluding national confidental information
Sanitized alarm
Countermeasure info
Store information
Event
Receives a possible countermeasure
Correlates data in order to find possible countermeasure
Alarm
Store alarm
Alarm
Yes
Countermeasure ?
Disssseminate alarm
Alarm
Store alarm
Alarm
Display alarm
Alarm
End

Figure 8. Validation scenario of SMP prototype.

A security event is sent form a Local Security System to the National GAMMA Security Management Platform (NGSMP) and displayed as alarm by the monitoring function of C&C module. The GAMMA operator decides to forward the alarm information to the EGCC.

Before forwarding, he "sanitizes" the information eliminating parts not permitted by national dissemination policies.

The sanitized alarm is sent through IDS module of NGSMP to European level and is displayed by the Monitoring function of the SMP instance of the European GAMMA Control Center.

Furthermore, using the Decision Support function, the GAMMA operator at NGSMP level send to the Local Security System a possible countermeasure for the security event.

VII. Conclusions

The most important concept of the GAMMA project, implemented by the federated architecture of the Security Management Platforms, is the sharing of security information between ATM stakeholders.

The SMP architectural vision enlarges the scope for cooperative management of ATM security while assuring controlled sharing of information, which is fundamental for its acceptance in a multinational context

The GAMMA concept opens the way for managing ATM security at European level, proposing (but not enforcing) recommendations on actions or measures to be taken at lower levels, in line with existing principles of national sovereignty and responsibilities over security issues.

The SMP is an enabler for the implementation of this concept, and can be adopted for the management of ATM security as well as the management of security in any federated environment (i.e. military domain)

References

[1] GAMMA Consortium – Description of Work – Part B – September 2013

[2] GAMMA Consortium, GAMMA CONOPS, The Ultimate ATM Security Framework, Newsletter, Issue No 1, pp. 2-3, 2015.

[3] GAMMA Consortium D6.3 Prototypes design and development, 1st release – March 2016

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

[5] Apache Kafka: www.kafka.apache.org.

[6] Data Fusion for Situation Monitoring, Incident Detection, Alert and Response Management, Shahbazian, E., Rogova, G., Valin, P, ISBN print 978-1-58603-536-5.

[7] Models for nuclear smuggling interdiction. IIE Transactions, Morton, D.P., Feng, P., J., S.K. 39(1), 3–14 (2007).

[8] Sonar tracking of multiple targets using joint probabilistic data association, T. Fortmann, Y. Bar-Shalom, and M. Scheffe, IEEE Journal of Oceanic Engineering, vol. 8, no. 3, pp. 173–183, July 1983