In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.

Cyber Threat Intelligence for Supporting ATM Security Management

Antonella Chirichiello[1], Claudio Porretti[1], Antonio Berardi[1]
[1]Leonardo, http://www.leonardocompany.com/
antonella.chirichiello@leonardocompany.com,
claudio.porretti@leonardocompany.com,
antonio.berardi@leonardocompany.com

Abstract

This paper presents the recent research advances in ATM (Air Traffic Management) industry showcasing the solution envisaged for the GAMMA Project and demonstrating how the cyber threat intelligence is used to support ATM security management.

1 Introduction

The cyber threat intelligence is a prevention tool for ATM security as it can help identify threat patterns and prevent attacks across Internet. The ability to gather cyber threat information from Internet and correlate it with data coming from ATM systems can enhance ATM security, lead the implementation of protection mechanisms and limit the impacts of incidents (Siu, Goh, & Lim, 2014).

This paper describes how the cyber threat intelligence can support the management of ATM security. We present the research advances in ATM industry showcasing the Security Management Platform (SMP) prototype developed for *Global ATM Security Management (GAMMA) Project* (GAMMA Project, 2016) co-financed by the Research Executive Agency of the European Commission within the Seventh Framework Programme (FP7). The project stems from the need to address new ATM threats due to the increased reliance on IT systems and automated flow of information across ATM systems. The goal is to develop solutions to ATM threats along with proposals for their implementation. Leonardo participates to GAMMA by contributing to the development of the SMP prototype providing Situational Awareness and Decision Support functionalities for the collaborative management of ATM security in a multi-stakeholder environment (AIAA, 2013). The SMP comprises Cyber Threat Intelligence module based on the *Leonardo Open Source Intelligence Platform* that provides information regarding emerging threats, as well as social and political contingencies that may have an impact on ATM security. The information feed resulting from the analysis of open Internet sources is used in the SMP as knowledge support tool to get a better understanding of security problems and dynamically adapt security countermeasures to fast changing threat scenarios (GAMMA Consortium, 2013).

In this demonstration paper, we describe the context of ATM security management and provide an overview of the GAMMA solution. Then, we drill down on the application scenario of ATM security at the national level and we introduce the Leonardo Open Source Intelligence Platform that provides the Cyber Security Intelligence capabilities in the SMP prototype. Finally, we describe the demonstration prepared to prove the concepts of the application scenario.

2 The Context: GAMMA Solution

Over the past decades in ATM industry we have assisted to the progressive and wide adoption of digital technologies to consolidate and enhance ATM operations. Several key aviation processes such as, airport baggage handling systems, flight information display systems and ATM information and communication technologies, make use of open systems architectures and internet-based flow of information. In the future, ATM will evolve to become a multitude of tightly interconnected heterogeneous systems exchanging lots of information (Siu, Goh, & Lim, 2014). The growing dependence of ATM on digitalization, though allows for an improved efficiency of ATM operations, inevitably introduces new forms of vulnerabilities that expose the entire ATM to cyber-attacks. Incidents resulting from cyber-attacks can affect the global aviation community or individual systems at many levels. These incidents could jeopardize communications and information exchanges between various ATM systems and stakeholders, impacting severely the safety and security of a country and damaging aviation business continuity. In this context, it emerges a clear need to implement a comprehensive framework for managing ATM security globally throughout a holistic approach that spans from threat prevention to the identification of security incidents and the efficient resolution of the ATM crises brought about by security incidents. This is the vision of the GAMMA Project (Porretti, Lahaije, & Kolev, 2016) that proposes a solution for collaboratively managing the ATM security in a multi-stakeholder environment through information sharing and exchange.
GAMMA recognizes that the most important concept for managing crises in ATM critical infrastructures is the sharing of security information between ATM stakeholders in order to generate prompt reaction to attacks. The sharing of security information like security alerts, countermeasures, security reports, is enabled thanks to a network of distributed nodes embedded within the ATM systems that act as interfaces to (ATM) internal and external security stakeholders. These nodes form a federated architecture that allows for managing security and disseminate information at three levels (Figure 1): *i*) *European level*, represented by the European GAMMA Coordination Centre (EGCC); *ii*) *National level*, represented by the National GAMMA SMP (NGSMP); *iii*) *Local level* represented by local security systems and the Local GAMMA Security Operation Centers (LGSOC).

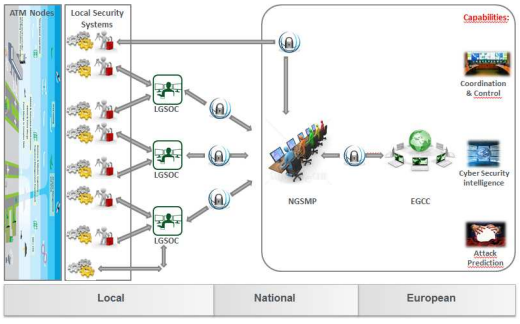

Figure 1: The GAMMA Solution

3 The National Security Management Platform

For the purpose of this paper, we focus on the National Level of the GAMMA solution. We assume that each local ATM system is provided with an event detector or a security system able to detect and manage locally a specific kind of possible threats. At the National level, all the information received from the lower (local) level are processed and analyzed by the SMP (Porretti, Lahaije, & Kolev, 2016). The SMP has been envisaged as an information sharing platform intended to provide a common overview on the status of ATM systems and a situational awareness to the Security operators operating in different ATM environments. Exploiting the National SMP, a Security operator has at its disposal in real time the following elements:

- status of each ATM system that the stakeholder decides to monitor;
- information on the status of the monitored systems that are connected with the SMP;
- information on the presence of a generalized status of alert (coming from both the analysis of the Internet data and the monitored systems);
- alert/alarm in case of anomalous situations notified by other countries, e.g., detected by an event detector or recognized by means of cyber threat intelligence information;
- expected impact of an undergoing attack;
- suggestions of the possible countermeasures that can be applied in case of alarm;
- synthesis of the information that can be distributed to the other stakeholders connected through SMP (with the relative level of confidentiality).

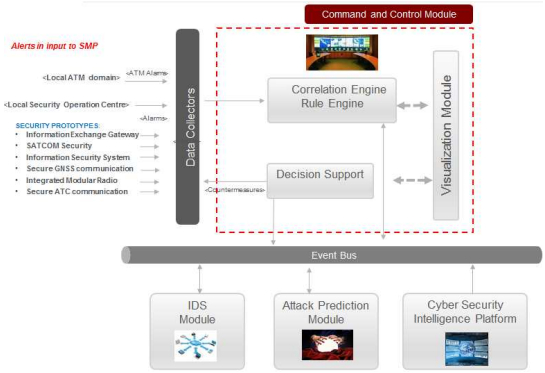

Figure 2: SMP Architecture

The SMP comprises several modules that implements situational awareness and decision support functionalities for supporting the coordinated management of ATM security (Figure 2). One module is the *Cyber Security Intelligence Platform* (CSIP) that provides cyber threat intelligence capabilities. The CSIP is based on the Leonardo Open Source Intelligence Platform that, by crawling and analyzing Internet sources (Web sites, blogs, IRC channels, forums, social networks, etc.) provides GAMMA operators with information regarding emerging threats to ATM security, as well as social and political contingencies that may have an impact on ATM security. The intelligence information feed is used as knowledge support tool complementing and integrating more traditional forms of intelligence, to get a better understanding of security problems and improve the ATM systems capabilities to dynamically adapt security countermeasures to fast changing threat scenarios.

The CSIP is an advanced environment for collection and real-time elaboration of heterogeneous information pertaining to the Internet (Open) Sources. The platform is based on a High Performance

Computer (HPC) specialized to carry out the acquisition and rapid processing of large quantities of data retrieved from Internet. The HPC is installed at Leonardo's facilities in Chieti (IT). The Internet sources to be monitored are selected based on criteria that consider both more specific aspects related to the investigation scenarios and the information needs pursued by the security operators w.r.t. the importance and risks exposure of the ATM infrastructures; as well as more general technical aspects related to IT systems and technologies deployed in the ATM infrastructures. The Monitored sources span from surface Web (Web pages, RSS feed, forum, blog, Social Networks like Facebook, Twitter, etc.) up to Deep/Dark Web (TOR, PAD, IRC channels, etc.). Other sources may be represented by information feeds and bulletins produced by cyber security vendors and Intelligence Operation Centers (IOCs) that enrich the analysis with data specific to cyber threats and vulnerabilities.

The CSIP provides the operators with tools for analyzing specific phenomena by detecting anomalous and suspicious behaviors in a semi-automated fashion. The investigation scenarios are described on the CSIP in terms of patterns, keywords and time intervals. Based on the configured scenarios, the GAMMA operator can acquire data from monitored Internet sources, identify patterns related to a particular phenomenon and extract entities using advanced automated mechanisms of crawling, indexing and searching. By exploiting data mining techniques and semantic-based engines, the processing of data allows for obtaining meta-level information that is preparatory for an in-depth analysis of the phenomenon of interest. The results of the processing are immediately submitted to analysts through a dedicated portal via visual tools called *Smart Views* (Figure 3). The Smart Views are advanced interfaces that can be dynamically configured to support the analyst in the analysis and identification of anomalies or incidents related to a topic of interest. Once relevant information is processed and potential risks are spotted, the GAMMA operator can produce a security report that can be sent to connected ATM domains, so that Security Managers can adopt possible countermeasures.

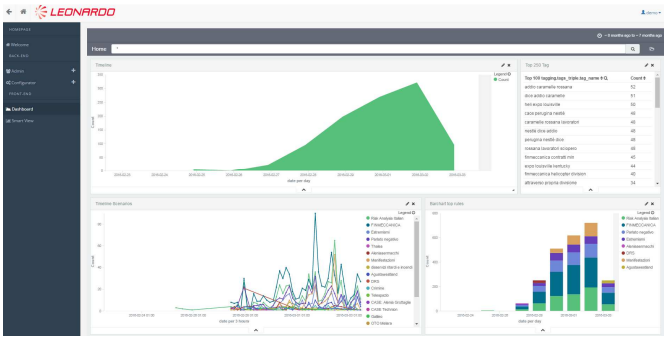

Figure 3: CISP Dashboard

The approach at the basis of CSIP (and consequently of SMP) that is used to build actionable intelligence items from the aggregated data is a balanced combination of automated and human-based techniques. On one hand, supervised automated mechanisms are exploited for collecting, indexing and categorizing huge amount of data that go behind the human processing capacity. On the other hand, the filtered data are fine-processed by the analyst to identify real threats and ultimately handle security incidents and reports. With the bulk of the work being carried out by automated processes, the operators can become much more productive and focus on more advanced concepts, such as identifying relationships between threats, reverse engineering attacks, real-time monitoring of suspicious activities in order to detect pre-planned attacks under preparation, and therefore enhancing the overall security of ATM infrastructures.

4 Demonstration Scenario

The demonstration scenario is originated from the validation of the SMP prototype for GAMMA with the purpose to validate the solution related to the following aspects: *i*) usefulness of obtaining information (at national level) about possible attacks on ATM assets by means of cyber threat intelligence tools & techniques; *ii*) correlation of the cyber threat information with other security alarms coming from local security systems to produce a cyber security reports about the status of ATM systems; *iii*) dissemination of security reports among ATM stakeholders to share security information and enhance the awareness on the security and status of ATM systems globally. The demonstration scenario comprises the following steps:

- A GAMMA operator at National level, using the CSIP, obtains information about a possible attack on ATM domain on national level.
- A sequence of alarms is generated by ATM local systems related to security events.
- The intelligence information and the sequence of alarms are correlated within the SMP in order to generate a detailed report about the identified threats. All sensitive information related to local and national level are sanitized and formatted for sharing purposes.
- The security report is then shared among the ATM stakeholders. The information about the identified attack and possible impact on the ATM systems can disseminated to other GAMMA National SMP either directly or through the EGCC at the European level, depending on collaboration policies and information sharing procedures established between nations involved within the GAMMA network.

For the sake of demonstration, we simulate the search and found of data on Internet sources about an attack against ATM infrastructures that has been recognized using the CSIP. Furthermore, we simulate some failures alarms messages from aviation systems. These alarms can be related to some ATM asset failures or generated by ATM systems (e.g., hijacking, general failure, etc.).

Acknowledgments. This work has been partially supported by GAMMA Project FP7-SEC-2012-2.2-2. A special thank goes to our colleagues Giovanni Micolucci, Lucio Brighella e Pietro Recchilongo who have contributed to the definition of the demonstration scenario and developed and integrated some of the demo components comprised in the SMP prototype, including the CISP module.

References

AIAA. (2013). *The Connectivity Challenge: Protecting Criticial Assess in a Networked World - A Framework for Aviation Cybersecurity*. An AIAA Decision Paper.

GAMMA Consortium. (2013). *Description of Work - Part B.*

GAMMA Project. (2016). October 2016, *Global ATM Security Management Project*: http://www.gamma-project.eu/.

Porretti, C., Lahaije, R., & Kolev, D. (2016). *A New Vision for ATM Security Management - The Security Management Platform*. Proceedings of International Conference on Availability, Reliability and Security (ARES) 2016.

Siu, M., Goh, D., & Lim, C. (2014). *Aviation Cyber Security: A New Security Lanscape.* Journal of Aviation Management.