SAWSOC

Situation Aware Security Operations Center

G. La Posta (FINMECCANICA), L. Romano (CINI)

ABSTRACT: *Security monitoring is a number one priority, since it is the pre-requisite for allowing system operation to continue also in the presence of attacks. A security monitoring facility produces three categories of outputs: 1) Alarms – Notifications to the personnel/machinery in charge of operating the monitored system/application of attacks that must be handled; 2) Remediation and Reaction triggers – Events that are sent to the personnel/machinery in charge of performing actions/procedures aiming at countering and/or mitigating the effects of attacks; 3) Actionable Evidence – Unforgeable electronic evidence of attacks, to be used in court. In order for security monitoring to be really useful, the aforementioned outputs must be made available in a timely fashion, i.e. in (near) real-time. A plethora of technologies exists, that individually represent a potentially effective building block of a real-time security monitoring facility, but – regrettably – they very much lack integration. While recently some achievements have been made, much is yet to be done, and further advancements in the convergence of physical and logical security technologies are very much needed. SAWSOC has proposed a novel approach – and a conceptual architecture – for real-time security monitoring of complex networked systems. The approach is to collect information at several architectural levels (namely: Physical, Network, Operating System and/or Virtual Machine, Data Base, Application, and Business Process) and to effectively correlate the diverse information flows, in order to timely and reliably spot malicious activities.*

1. Introduction

Security has become one of the major topics in contemporary societies. While facing new security risks and challenges like e.g. international terrorism, crime, climate change and economic crises, an increased concern for security can generally be observed among many European populations. Increasingly, attempts are made to 'produce' security in a primarily technological way.

Technologies for implementing security services in the physical and in the electronic domain are both stable and mature, but they have been developed independently of each other.

Security Operations Center (SOC) technology has improved significantly, but SOC solutions have typically been developed using vertical approaches, i.e. based on custom specific needs. Other key security technologies (such as: Forensic support, Identity Management, Building Automation, and Video Surveillance) have also made dramatic improvements, but there is still a limited capability of performing complex correlation on security relevant data.

The fragmentation of security approaches is perceived by citizens with confusion, disorientation, and fear. This discomfort is also amplified by the relatively high rate of false alarms.

SAWSOC has brought about a significant advancement in the convergence of physical and logical security.

SAWSOC enhanced awareness capabilities allow accurate, timely, and trustworthy detection and diagnosis of attacks, which ultimately results in the achievement of two goals of paramount importance, and precisely:

1. guaranteeing the protection of citizens and assets;
2. reducing the perception of fragmentation of security approaches, thus improving citizen's perception of security.

2. Project Objectives

SAWSOC objective was to identify, implement, and validate techniques for achieving the convergence of physical and cyber security solutions. More in detail, the project aimed at:

- Advancing the state of the art of some of the key physical and logical security technologies;
- Developing techniques for correlating physical and logical security services, to achieve a consistent view and to be able to produce an irrefutable record of who did what, where, and when;
- Implementing those techniques in a Situation AWare Security Operations Center (SAWSOC) i.e. an integrated platform for providing sophisticated security services combining in a modular way diverse information from multiple data sources;
- Demonstrating and validating the proposed techniques and the framework by performing a thorough experimental campaign with respect to three substantial case studies.

3. Use Cases

SAWSOC design has been driven by three real use cases that were carefully selected with two objectives:

1. Capturing the diversity of the requirements;
2. Improving the perception of security by citizens.

The first use case, namely MIARCI (Maintenance Impacts and Attack Recognition on Critical Infrastructures), was provided by ENAV, the Italian air traffic control provider.

The SAWSOC platform implemented correlation techniques that allowed the protection system to discriminate between malicious attacks and alerts related to maintenance actions.

The second use case is called EPDCI (Energy Production and Distribution Critical Infrastructure). It

was provided by IEC, the largest electric utility in Israel.

SAWSOC successfully correlated logical and physical information, and ultimately supported the decision making process on which dependable operation of the energy CI relies, particularly in the presence of sophisticated attacks.

The third use case is called CES&S (Crowded Events Safety & Security) and it was provided by Comarch, the Polish SME in charge of security management at the Cracovia stadium.

The use case dealth with the protection of people attending an event at the stadium. SAWSOC provided important security features, such as early identification of abnormal behavior and improved detection of unauthorized access.

4. Main Achievements

At the end of the project activities all the phases (namely: use case analysis, technology review and gap analysis, components implementation, platform implementation, demo & validation) have been successfully completed. More in detail:

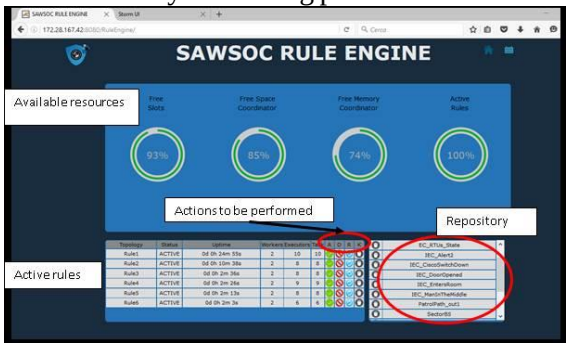
- The three SAWSOC application domains were thoroughly analysed, and some challenging misuse cases were identified, which represented some of the most relevant security issues affecting systems in the reference domainsof the project.
- A thorough technology review update was carried out, with respect to the key technologies on which the SAWSOC platform relies, namely: Security Information and Event Management (SIEM), Digital forensics, Security Operation Center (SOC), Physical Security Information Management (PSIM), Building Automation, Identity Management, and Video Surveillance. The study highlighted that currently available

products are still far from achieving real convergence between physical and logical security.

- The architecture of the SAWSOC platform was designed. This was the result of a collaborative process during which both general and use case specific requirements were taken into account. A high level view of the SAWSOC architecture is presented in Figure 1.
- The key components of the SAWSOC architecture were implemented.

  The *Correlation Engine* is the component in charge of the event diagnosis process. It correlates a large amount of security relevant events/information from the physical and the electronic domain. The attack diagnosis process is driven by correlation rules that aggregate the parameters of attack symptoms, such as the attack type, the target component and the temporal proximity. Alerts are generated only when the correlation among such symptoms indicates a potential attack, thus exhibiting low false positive rates and improved detection capability. It consists of two main parts:
  - the data collection framework in charge of managing the high heterogeneity of formats and data sources.
  - the distributed processing engine, relying on real time Complex Event Processing (CEP) technology, to ensure high performance, scalability, and resilience.

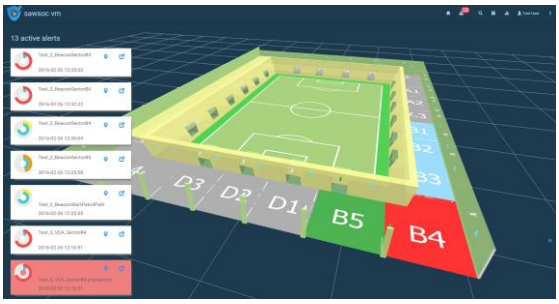
  The *Rule Engine*, including Signature Based Support (SBS) and the Anomaly Based Support (ABS), provides the logical rules to be followed by the Correlation Engine. In the approach taken by the SAWSOC platform, SBS and ABS cooperate to detect a wide variety of possible attacks to the systems being protected.



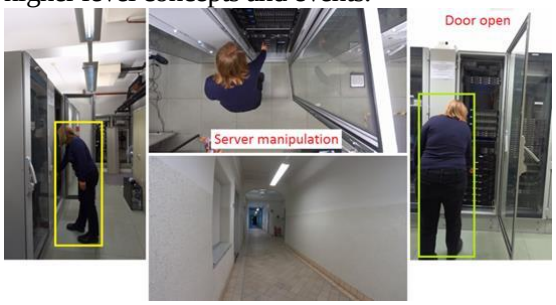
The *Forensic Module*, provides a set of services that enables the end user (SOC operator) to back trace from a security breach to the complete list of events that led to the incident. The module ensures that the events and their associated logs are stored in a "forensically valid" manner. It supports processes that ensure, to the greatest extent possible, that the event data will be acceptable as evidence in court.

The *Identity & Credential Management system*, manages trusted, secure credentials for user and device authentication, as well as (digital) event signing within the SAWSOC platform.

The *Visualization Module*, implements the User Interfaces of the SAWSOC platform offering functionalities like e.g.: alarm notifications, alarm details presentation, actions list presentation, alarm statistics, 3D modelling of protected area, and more.



The *Video Content Analysis* component receives the inputs from video surveillance and fuses the lower level results from video surveillance into higher level concepts and events.



- The components were integrated into the SAWSOC platform which was then validated with respect to the three different use case.
- Three demos (one for each Use Case) were given at the final project workshop, which was held in Kracow on the 07 April 2016.

5. Social aspects and perspectives

The development and implementation of convergent security systems for protecting critical infrastructures confronts its developers, providers, users and others affected with a number of technological,

administrative and organisational challenges. Moreover, potential (side-) effects on the perceptions, the attitudes and the behaviour of people concerned with a new security system are of relevance. Reactions in interaction with a given technology may result and impact on its functionalities or even worse, thwart the intended purpose and proper operation. To this end, a socio-scientific evaluation of the attitudes and perceptions of stakeholders involved in the development as well as affected by the outcomes of convergent security systems accompanied the technological development in the SAWSOC project. In summary, employees in the private security sector generally hold positive attitudes towards convergent security systems. The perception of convergent security systems is not limited to functional aspects of the systems. Moreover, socio-psychological factors are amongst the most important determinants for the perception of convergent security systems. To this end, concerns regarding privacy issues and the protection of personal data are associated with the acceptance or refusal of such systems. Finally, socio-ecological aspects of the working environment have a bigger impact on feelings of security than technological security solution do.

5. Conclusions

The SAWSOC FP7 project started in November 2013 to implement and validate techniques for achieving the convergence of physical and logical security technologies.

SAWSOC has been designed and its dependability has been tested considering three use cases:

1. Maintenance Impacts and Attack Recognition on Critical Infrastructure(MIARCI).
2. Energy Production and Distribution Critical Infrastructure(EPDCI).
3. Crowded Events Safety & Security (CES&S).

The final result is a prototype able to demonstrate the improvement that can be achieved in the field of real-time security monitoring of complex networked systems through effective convergence of physical and logical security technologies.

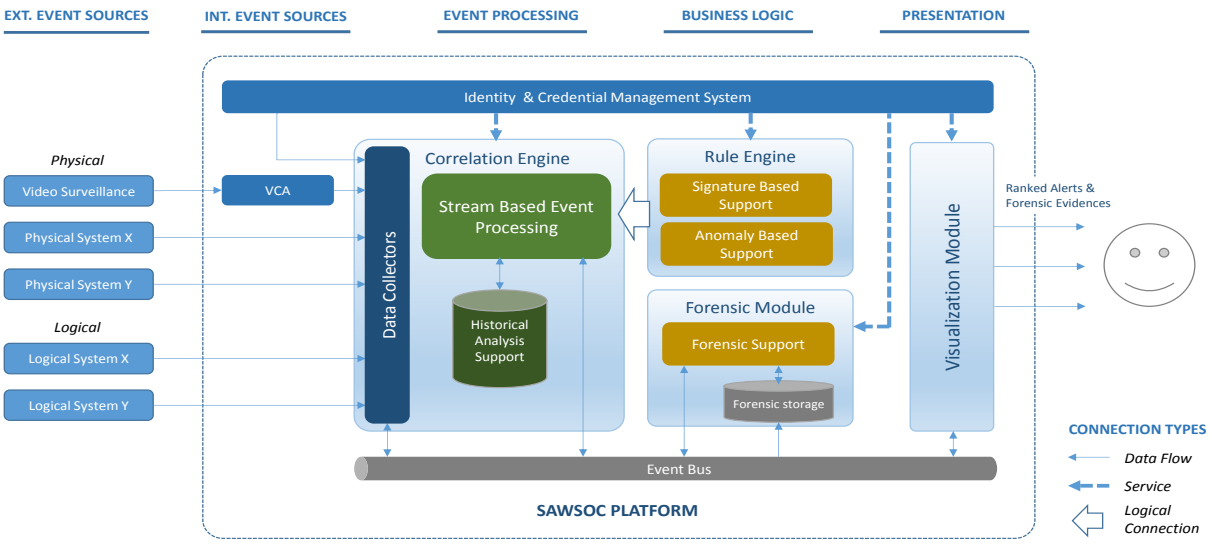


Figure 1 : SAWSOC platform architecture

Contact details

SAWSOC WebSite: http://www.sawsoc.eu/

Project Coordinator: Giuseppe La Posta (FINMECCANICA): giuseppe.laposta@finmeccanica.com

Technical Coordinator: Luigi Romano (CINI): luigi.romano@uniparthenope.it