Enhancing SIEM technology for protecting Critical Infrastructures

Luigi Coppolino
Epsilon Srl

Salvatore D’Antonio
CINI

ETSI Security Workshop Programme Committee
18 – 19 January 2012, Sophia Antipolis, France

www.massif-project.eu

Project funded by the European Commission ICT work programme 2009 (FP7-ICT-2009-5)
Roadmap

- Critical Infrastructures cyber-security
- SIEM technology: SOTA review
- The MASSIF project
- Case Study from the MASSIF project
- Wrap up
The European Commission (EC) defines an “infrastructure” as “Critical” when it is so vital that, if it is disrupted or destroyed, this would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.


The definition stated by the USA is very close to that.

- Source: GAO, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, USA, March 2004
CI technology shift

Traditional CIs were intrinsically secure systems

- Were largely based on special purpose devices
- Consisted of individual sub-systems, which operated almost in isolation
- Used dedicated (as opposed to shared) communication links
- Relied on proprietary (as opposed to open) communication protocols
- Commercial-Off-The-Shelf (COTS) components are being massively used for implementing SCADA systems
- Subsystems are being connected using the infrastructure of the corporate LAN, or even WAN links, possibly including the public Internet, as well as wireless/satellite trunks
- Open communication protocols are being increasingly used
  - exposing SCADA systems to the same vulnerabilities of general IT systems
- Wireless Sensor Networks (WSNs) have become an integral part of virtually any CI
Evidence is showing that Critical Infrastructures (CIs) are already exposed to Cybersecurity attacks and they will be even more so in the future.
A Security Information and Event Management (SIEM) solution effectively combines elements of security information management with security event management.

**SIEM solutions typically correlate, analyze and report information from a variety of data sources**, such as network devices, identity management devices, access management devices, and operating systems.

This bundling of services has become common across the security products market as vendors offer “one stop solutions” which allow the end user to provide real-time analysis of security alerts.

One of the main features of these solutions is their advanced **log management** capabilities.

Log management is a process of dealing with large volumes of computer generated log messages, which are commonly referred to as audit records or event-logs.

In general, Log management covers collection, aggregation, retention, analysis, searching and reporting.

The **key issues** with log management tend to be **the sheer volume of the log data and the diversity of the logs**.
There are a number of leading providers in this area, most notably ArcSight, RSA, and IBM (Q1 Labs).

- **ArcSight** are viewed by most as the market leader in this area with their Enterprise Threat and Risk Management (ETRM) Platform.

- **IBM (Q1 Labs)** Provides log management, event management and behavioral analysis for networks and applications. A weakness of the product is its lack of detailed integration with SAP.

- **RSA’s enVision** appliance provides a combination of SIEM and log management to its end users. It has a very powerful correlation engine, is quick to install and easy to configure.

- **OSSIM** is released under the GPL license by AlienVault. It is the most widely used Open Source SIEM.
MASSIF facts

- **IP project** funded by the European Union FP7 Information Society and Media.
- **ID:** 257475
- **Call ICT 5:** Objective ICT-2009.1.4: Trustworthy ICT
- **Project start:** October 2010
- **Duration:** 36 months
- **Overall budget:** ~ 6 Mio. €
- **Project Coordinator:** Atos Origin
- **12 different organisations** from 7 countries.
Why MASSIF?

- Management of incidents and events (SIEM)
  - Near-real time notification;
  - Proactive management of incidents and events.

- Limitations of current SIEM solutions:
  - Restriction to infrastructure
  - Inability to interpret events and incidents from multiple system layers (application, network, physical, ….)
  - Inability to provide high degree of trustworthiness or resilience in the event collection environment
  - No scalability to provide posture of the environments when considering global deployment of ICT infrastructure.
MASSIF Objectives

- Development of a new generation SIEM framework for service infrastructures.

- Security event processing:
  - intelligent
  - scalable
  - multi-level
  - multi-domain

- Predictive security monitoring.

- Trustworthiness & resilience of event collection framework
MASSIF scenarios

Massif project presentation

- MASSIF results will be demonstrated in:
  - Four field scenarios:
    - Olympic Games IT infrastructure
    - Mobile phone based money transfer service
    - Managed Enterprise Service Infrastructures
    - Critical infrastructure process control

- Existing SIEM solutions:
Case Study from the MASSIF Project
Setting up the scene

A dam used for hydropower generation

UNWANTED SOLICITATIONS TO THE TURBINES MAY HAVE DRAMATIC EFFECTS (SAYANO-SHUSHENSKAYA, SIBERIA, 75 DEAD).
Misuse Case Overview: Access

The attacker, an unfaithful employee in charge of cleaning premises, has stolen administrative credentials for accessing the machines in the control room.

He compromises the sensor so to hide changes in the flow rate.

The malicious user accesses the Control Room by using his RFID badge.

The user also logs into a computer with administrative (stolen) credentials.
Misure Case Overview: Trigger

- The attacker cuts-off communications between the hydropower station and the control machine
  - e.g. by installing a software dropping away packets sent by the hydropower station to the control machine.

It is worth noting that this would also PREVENT the packets sent from sensors in the hydro station from reaching the SIEM

- The attacker sends an open-gate command to discharge the reservoir through the penstock.
  - The compromised sensor doesn’t indicate an increase in the flow rate level in the penstock
  - Turbines vibration level do not reach the control station due to the broken channel => the Control Station continues to release water in the penstock
The overstressed turbines finally break down resulting in damages and injuries.

UNWANTED SOLICITATIONS TO THE TURBINES (SAYANO-SHUSHENSKAYA, SIBERIA, 75 DEADS).
Thanks to the GET framework heterogeneous events are easily collected and feed in a common Format to the event correlation engine.

The huge amount of data reaching the MASSIF engine can be easily managed thanks to the highly-scalable, dependable and multi-level correlation provided by MASSIF.
Misuse Case Detection with MASSIF
Advanced SIEM framework (activity 5)

In spite of the communications cut-off, MASSIF resiliency guarantees the delivery of security-relevant events to the SIEM.

1) Preparation
   - Steal admin credentials
   - Compromise sensors

2) Access
   - Log into the room with a legitimate RFID badge
   - Log into the system with administrative credentials

3) Misuse
   - Interrupt hydropower station to control room communications
   - Issue an open gate command

4) Failure
   - The overstressed turbines break-down
Misuse Case Detection with MASSIF

Predictive Security Monitoring (Activity 4)

Security Goals
- Formal description of system behavior and security requirements

Monitoring Rules
- Admin activities require admin presence
- Inbound and outbound flows in the hydropower station should be equal
- Variation of the dam basin water level should be a function of the incoming and outgoing water flows

Control Station

2) Access
- Unauthorized attempts
- Intrusion attempts
- Unauthorized access attempts

3) Misuse
- Unauthorized control attempts
- Intrusion attempts
- Unauthorized access attempts

4) Failure
- The system is breached

Massif project presentation
Misuse Case Detection with MASSIF

The stress level of turbines is under control, and failures and injuries are avoided thanks to the decision support provided by MASSIF proper reaction and remediation initiatives can be taken.

1) Preparation
   - Steal admin credentials
   - Compromise sensors

2) Access
   - Log into the room with a legitimate RFID badge
   - Log into the system with administrative credentials

3) Misuse
   - Interrupt hydropower station to control room communications
   - Issue an open gate command

4’) Reaction/Remediation

Failure
   - The overstressed turbines break-down
Realistic Testbed – 2/2

Two pumps allowing variable flow levels

- Seepage Channel
- Penstock Channel
- Reservoir
- Afterbay
- Control Station
Conclusion

- MASSIF will help to increase the trust in processing of events provided by various sources and various layers.

- OSSIM and Prelude are building blocks that will be used in MASSIF studies.

- The research results will be adapted to several fields: Olympic games, Critical infrastructure process control, money transfer with mobiles, and Enterprise Service Infrastructures.
Contacts

Luigi Coppolino

luigi.coppolino@epsilonline.com
Mobile: +39-339-6218570

Salvatore D’Antonio

salvatore.dantonio@uniparthenope.it
Mobile: +39-329-0730003
Massif Contacts

- **Project Coordinator**
  Pedro SORIA  
  pedro.soria@atosorigin.com

- **Scientific Coordinator**
  Roland RIEKE  
  Roland.Rieke@sit.fraunhofer.de

- **Technical Coordinator**
  Hervé DEBAR  
  herve.debar@telecom-sudparis.eu

- **Project Website:**  
  http://massif-project.eu
Thank you for your attention!