RaSIEM 2013: call for participation

The MASSIF consortium cordially invites you to the *2nd International Workshop on Recent Advances in Security Information and Event management* **(RaSIEM 2013)**. This workshop will be hosted by the *8th International Conference on Availability, Reliability and Security* (ARES) on **September 4th 2013** at the **University of Regensburg**, Germany.

This workshop proposes 6 peer reviewed oral presentations on works for advanced Security Information and Event Management (SIEM) systems, 2 invited presentations and some demonstrations from the MASSIF project.

This workshop is organized by the MASSIF project. MASSIF (*MAnagement of Security information and events in Service InFrastructures*) is a collaborative project co-funded under the European Commission's FP7 ICT Work Programme 2009 (FP7-ICT-2009-5). It is aligned with the objective ICT-5-1.4 - Trustworthy ICT.

Some links

- Host conference website (ARES 2013): http://www.ares-conference.eu/
- Host conference program: http://www.ares-conference.eu/conf/index.php?option=com_content&view=article&id=78&Itemid=107
- Registration: http://www.ares-conference.eu/conf/index.php?option=com_content&view=article&id=57&Itemid=97
- MASSIF project website: http://www.massif-project.eu/

Workshop presentation

The management of events and incidents is one of the cornerstones for any service. Traditionally, event management frameworks are responsive. The SIEM (Security Information and Event Management) approach enables near-real time event management as well as proactive management of security incidents and events for IT infrastructures. However, the SIEM solutions available commercially are not able to interpret high-level data from the service view or the business impact view. Another limitation of SIEMs is related to scalability. Indeed, current solutions are limited since they depend on centralized rule processing performed on a single node.

One of the most challenging domains for SIEMs, but not only, is the protection of critical infrastructures. Over the last few years, there has been growing understanding of security risks related to (targeted) cyber-attacks against critical infrastructures in all sectors (dams, energy, transport, etc.). Critical infrastructure networks are very different in comparison to other IT infrastructures. Most of the endpoint actors are machines rather than people, their malfunction can have immediate physical consequences, and they are more likely to be targeted by malicious adversaries. The protection of these networks faces several challenges, such as:

- Recognizing real threats in the multitude of daily alerts.
- Ensuring data source reliability.
- Managing data from heterogeneous devices and networks.
- Correlation of highly heterogeneous data to identify threats.
- Ensuring the resilience against all hazards

Workshop Agenda

9h30 S1. RaSIEM invited presentation 1

Session chair: Elsa Prieto (Atos)

- **Elastic SIEM: Elastic Detector integrated with OSSIM**

  Presenter: *Pasquale Puzio (Secludit and* EURECOM*).*

  Abstract New cloud IT infrastructures bring new security challenges, brought by elasticity, programmability and multi-tenancy. The goal of Elastic Detector is to be an advanced security probe that collects cloud infrastructure events to a SIEM. Elastic Detector does a first set of security analysis on virtual servers, the cloud software stack and the virtual firewalls and networks. Correlation with other security events, for example brought by traditional (e.g. non-cloud) IT infrastructures, are then performed at the SIEM level.
  The goal of this presentation is to make an overview of the new security challenges brought by cloud infrastructures and to show how Elastic Detector addresses them. A demo of an integration of Elastic Detector with OSSIM will be shown in the context of security management of a public cloud infrastructure.

10h30 Coffee Break

11h00 S2. RaSIEM session 1

Session chair: Roland Rieke (Fraunhofer-SIT)

- **A Scalable SIEM correlation engine and its application to the Olympic Games IT infrastructure**

  Authors: *Valerio Vianello (UPM), Vincenzo Gulisano (UPM), Ricardo Jimenez-Peris (UPM), Marta Patiño-Martínez (UPM), Rubén Torres (Atos), Rodrigo Díaz (Atos), Elsa Prieto (Atos).*

- **Reconsidering Intrusion Monitoring Requirements in Shared Cloud Platforms**

  Authors: *Kahina Lazri (Orange labs), Sylvie Laniepce (Orange labs), Jalel Ben-Othman (L2TI)*

11h40 S3. RaSIEM session 2

Session chair: Roland Rieke (Fraunhofer-SIT)

- **The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems**

  Authors: *Igor Kotenko (SPIIRAS), Olga Polubelova (SPIIRAS), Igor Saenko (SPIIRAS), Elena Doynikova (SPIIRAS).*

- **Addressing security issues of Electronic Health Record systems through enhanced SIEM technology**

  Authors:*Cesario Di Sarno (University of Naples Parthenope), Valerio Formicola (University of Naples Parthenope), Mario Sicuranza (ICAR-CNR), Giovanni Paragliola (ICAR-CNR)*

12h30 Lunch Break

14h00 S4. RaSIEM session 3 - Anomaly detection

Session chair: Mohammed Achemlal (Orange Labs)

- **Experiences and Challenges in Enhancing Security Information and Event Management Capability using Unsupervised Anomaly Detection**

  Authors: Stefan Asanger (University of Cape Town), *Andrew Hutchison (T-Systems International)*

- **Fraud Detection in Mobile Payment Utilizing Process Behavior Analysis**

  Authors: Roland Rieke (Fraunhofer SIT), Maria Zhdanova (Fraunhofer SIT), Jürgen Repp (Fraunhofer SIT), Romain Giot (Orange labs), Chrystel Gaber (Orange labs)

14h40 S5. RaSIEM invited presentation 2

Session chair: Mohammed Achemlal (Orange labs)

- **Contemporary SCADA system, their design and usage**

  Presenter: *Gunnar Björkman (ABB)*

  Abstract Computerized control systems, so called Supervisory, Control and Data Acquisition (SCADA) systems, are regularly used for the supervision and control of the electrical grid. This type of control systems represents a mature technology that has been used since more than 40 years. They can be seen specialized SIEM systems dedicated for a specific process. Among very many other applications, the Event and Alarming Handling functionality is an important part of each SCADA system where a very high amount of events are collected in a short time and where the system must correctly filter, analyze and alert the operators in an intelligent way. Examples when the alarming function has failed and the very severe consequences of such failures will be given.

  Another essential part of a SCADA system is the model-based analysis of incoming process events. SCADA systems includes a mathematical model of the supervised process which is used to make advanced, higher level alarming and to make predictions of the future process states and recommendations for how to operate the process to avoid potential disturbances. In order to make this model-based analysis the process models must be created and maintained. This Data Engineering process is also an important, and not to be ignored, part in the use of SCADA systems.

  This presentation will give an overview of contemporary SCADA system for the electrical grid, a short description of their evolution, their design and usage. Special emphasis will be given to the event and alarming functionality, the model based analysis and to data maintenance.

15h40 Coffee Break

16h00 S6. Demonstrations

Session chair: Roland Rieke (Fraunhofer-SIT)

- **Mobile Money Transfer Scenario**

  Presenter: *Chrystel Gaber (Orange labs)*

  Abstract: The field of MMT is a growing market segment, particularly in developing countries where banking systems may not be as dense or available as in developed countries. For example, M-Pesa, which was launched in 2007 in Kenya, displayed in December 2011 about 19 million subscribers, namely 70% of all mobile subscribers in Kenya. Orange Money is deployed in 10 countries and gathers around 14% of the mobile subscribers of these countries. In such services, transactions are made with electronic money, called mMoney. The users can convert cash to mMoney through distributors and use it to purchase goods at merchants, pay bills or transfer it to other users. Like any other money transfer service, this service is exposed to the risk of money laundering, i.e., misuse through disguising illegally obtained funds to make them seem legal, and more generally fraud risk that implies any intentional deception made for financial gain.

  The demonstration's objective is to highlight the results of the European FP7 project MASSIF in terms of components integration and their adaptation to the Mobile Money Transfer Scenario. All MASSIF modules are illustrated from the collection of events to the enforcement of countermeasures after a fraud is detected and a component based on process behavior analysis is highlighted.The misuse case showcased is related to money laundering and in particular, a specific use of mules. More details about the misuse case and the way it is

detected are detailed and discussed in the article “Fraud Detection in Mobile Payments Utilizing Process Behavior Analysis” also presented in the RaSIEM workshop.

- **Critical Infrastructure Protection Scenario demonstration synopsis**

  Presenter: *Valerio Formicola (University of Naples Parthenope)*

  Abstract: As a consequence of the technology shift and of new economical and socio-political motivations, coordinated and targeted cyber-attacks to Critical Infrastructures (CIs) are increasing and becoming more sophisticated. Mostly, such infrastructures rely on legacy Supervisory Control And Data Acquisition (SCADA) systems that have been designed without having security in mind - originally they were isolated proprietary systems - and that are managed by people with good skills in the specific application domains, but with very limited knowledge of security.

  Security of SCADA is traditionally approached by reusing systems designed to protect solely Information Technology (IT) based infrastructures. One of the most effective solutions is represented by Security Information and Events Management (SIEM) systems. Unfortunately, according to the National Institute of Standards and Technology (NIST), securing a Critical Infrastructure is very much different from protecting solely IT-based infrastructures, hence traditional SIEMs are often ineffective for CIs protection.

  This demo is aimed at demonstrating the usage of the MASSIF framework to overcome some of the limits of traditional SIEM technologies. In particular the demo shows how the interaction among most of the MASSIF components, allows to deal with internal attacks by processing heterogeneous events coming from a number of data sources.

  The demonstration is operated with respect to a very challenging case study, namely the control system of a dam. Since September 2009 dams are classified as critical infrastructures and thus they are being increasingly monitored against malicious faults. Some of the main MASSIF framework features demonstrated by the demo include: i) correlation of heterogeneous data sources; ii) attack prediction; iii) cyber-physical convergence; and iv) decision support for reaction and remediation.

17h00 S7. Closing session

- **Summary of the MASSIF project and link to other SIEM advances**

  Presenter: *Elsa Prieto (Atos)*

17h00 End of event

Workshop Chairs

Mohammed Achemlal, France Télécom-Orange - France
Romain Giot, France Télécom–Orange - France
Chrystel Gaber, France Télécom–Orange – France
Elsa Prieto Perez, Atos - Spain
Roland Rieke, Fraunhofer SIT-Germany

Program Committee

Luigi Coppolino, Epsilon - Italy
Andrey Chechulin, SPIIRAS – Russia
Rodrigo Diaz Rodriguez, Atos – Spain
Gustavo Gonzales Granadillo, TELECOM SudParis - France
Igor Kotenko, SPIIRAS – Russia
Andrew Hutchison, T-systems – South Africa
Luigi Romano, University of Naples - Italy
Maria Zhdanova, Fraunhofer SIT - Germany