ECOSSIAN - EUROPEAN CONTROL SYSTEM SECURITY INCIDENT ANALYSIS NETWORK

Newsletter

November 2016 - Issue 5

Ecossian

Message from the Coordinator

Within the last months, major specification work has been finished and implementations of ECOSSIAN architectural component functions and interfaces are in the phase of becoming completed and ready to be demonstrated and evaluated. Actually, special attention is drawn to the integration of all the relevant components for supporting real-life demonstrations. Our expectations are very promising, as component's integration within laboratory setups was done successful. Based on these achievements, first evaluation was done comparing results with the requirements set-up by the consortium and approved within several stakeholder workshops. This evaluation work will be continued based on the demo installations. In July, the project has become evaluated by the European commission, with involvement of external reviewers, a second time successfully. Following that review, a summary of the results achieved within the first two project years as well as the public deliverables have been made available at the ECOSSIAN Web site (http://ecossian.eu/published-results/deliverables).

In this Issue

Technical Meeting Rome, Italy

From 21st—22nd September 2016 , the ECOSSIAN consortium met for a technical face-2-face meeting in Rome, Italy. The meeting was hosted by partner *Poste Italiane*. Besides discussions concerning the technical work for the upcoming months, the meeting was mainly dedicated to the preparation of the Italian National demonstration, which will take place on 8th November in Rome. On the first day of the meeting, a technical workshop for the Italian demonstration was organized by the demo lead *Cassidian Cybersecurity SAS*. On the second day the concept of the Italian demonstration was presented to the entire ECOSSIAN consortium and feedback was provided. Additionally, rehearsal and training sessions on the ECOSSIAN components involved in the national demonstrations took place. Another focus was on the legal compliance of the ECOSSIAN solution, especially the possible use of personal data, and on the planning of dissemination activities for the last project period. Discussions on the 3rd ECOSSIAN workshop were held and possible events were evaluated. Last but not least the compliance of several requirements with the ECOSSIAN system was discussed.

Publicly available project outcomes

A number of publications have been realized in the past couple of months. The latest publication of 2016 "**A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing**" as well as many other publications can be found on the project website at www.ecossian.eu.

Key Data:

Start Date:	1 June 2014
End Date:	31 May 2017
Duration:	36 months
Project Reference:	607577
Project Costs:	€ 13.196.720,61
Project Funding:	€ 9.224.459,00

Consortium: 19 partners (9 countries)

Project Coordinator: Dr. Klaus-Michael Koch
coordination@ecossian.eu

Technical Leader: Mag. Helmut Kaufmann, MSc
helmut.kaufmann@airbus.com

Project Website: www.ecossian.eu

LinkedIn

FOLLOW US ON twitter

https://twitter.com/FP7_ECOSSIAN

ECOSSIAN - EUROPEAN CONTROL SYSTEM SECURITY INCIDENT ANALYSIS NETWORK

Newsletter

November 2016 - Issue 5

Ecossian

ECOSSIAN National and European Demonstrations

The demonstrations will be one-day events. Each demonstration is based on the scenarios that have been defined and on the findings from the evaluation experiments. The demonstrations will provide an explanation of the capabilities of the integrated system deployed in realistic operational contexts. They will prove how the ECOSSIAN system can be used, its main features, the global workflow, from threat detection within an O-SOC to threat mitigation at the national/European level (N-SOC/E-SOC), and how information will be shared between CIs and governmental stakeholders. The demonstration will target a mixed audience and therefore will alternate between technical descriptions and high-level explanations and conclusions. Feedback and an evaluation from the participants will be collected after the demonstrations. Also, proposals for improvements of the ECOSSIAN system will be taken into account in the evaluation and recommendation report. The performance of the ECOSSIAN system is evaluated systematically along a set of criteria which addresses 3 different perspectives of the system and its modules: (1) the effectiveness of the system in the tested threat cases, (2) the inherent qualities of the system (e.g. on usability), and (3) the expected societal and political impact of the system.

Three National demonstrations have been planned. One in ***Italy*** with ***Poste Italiane*** being the main lead, one in ***Ireland*** where ***Bord Gais*** as a gas network provider leads the demonstration, and one in ***Portugal*** with ***Infraestruturas de Portugal, INOV INESC INOVACAO—Instituto de Novas Tecnologias*** and ***Ministério da Justiça*** as key players. A **final European demonstration** will be done involving several partners and all layers presented in the full technical solution. It will be performed in ***Cassidian Cybersecurity SAS*** premises in Elancourt, near Paris, ***France***.

Italian Demonstration—Early Warning of Attacks on Financial Infrastructure:

Attack description: An employee PC gets infected with Advanced Persistent Threats (APT), which spreads to a server that provides a financial service. A hidden malicious script injected by the attacker is used to spread the malware in the company's network. APT leaks information about this service or disrupts the service.

If the attack was successful, the attacker will obtain sensitive information about critical infrastructures, with the threefold goal of service disruption, espionage and data corruption. The attack would be detected by ECOSSIAN sensors (Honeypot & BroLHG IDS) and an incident report will be generated by the SIEM and securely transferred to an N-SOC for further analysis and correlation. The concerned end-user is Poste Italiane, a national and international benchmark in postal, courier, logistics, finance, insurance, and the mobile phone market segments.

Irish Demonstration—Detection of Attack on Gas Provider:

Attack description: There will be a man-in-the-middle between the Remote Terminal Unit (RTU) of Pressure Reduction Equipment and the SCADA servers. False telemetry readings will indicate a gas leak.

If the attack was successful, the block valves will be closed by the Grid Operator. The consequence will be an isolation of the town and electricity power station from the gas network. The attack would be detected by ECOSSIAN sensors (ICS Monitor) by comparing data sent from the RTU with data received by the SCADA servers. The involved end-user is Bord Gais whose principal activities are gas procurement & supply, as well as the operation of the gas transportation network.

Portuguese Demonstration—Support for Forensic Analysis of Attack on Transportation Infrastructure:

Attack description: A Network Intrusion through social engineering and a discovery process (network scanning) will be simulated in order to find exploitable vulnerabilities on key network equipment and systems. Forged speed limitation orders will cause major service disruption. Forged packets perceived as an actual obstacle will take control of a specific train. The denial-of-service on the CCTV system and the Train-to-Ground voice communications will be a consequence. The intrusion will be detected through a significant statistical deviation on the firewall logs. ECOSSIAN sensors will detect port scans from compromised workstations and injected packets. Finally, the forged requests will be detected through comparison of logs between emitting applications and print queues. The involved end-user will be Infraestruturas de Portugal who is managing the infrastructure of the Portuguese Railway System.

Dates and venue of demonstrations

- **Italian National Demonstration:**
  8th November 2016, Poste Italiane, Rome, Italy
- **Portuguese National Demonstration:**
  18th January 2017, Infraestruturas de Portugal, Lisbon, Portugal
- **Final European Demonstration:**
  March 2017, Cassidian Cybersecurity, Elancourt, France
- **Irish National Demonstration:**
  Date to be fixed.

Key Data:

Start Date:	1 June 2014
End Date:	31 May 2017
Duration:	36 months
Project Reference:	607577
Project Costs:	€ 13.196.720,61
Project Funding:	€ 9.224.459,00

Consortium:	19 partners (9 countries)
Project Coordinator:	Dr. Klaus-Michael Koch coordination@ecossian.eu
Technical Leader:	Mag. Helmut Kaufmann, MSc helmut.kaufmann@airbus.com
Project Website:	www.ecossian.eu

LinkedIn

FOLLOW US ON twitter

https://twitter.com/FP7_ECOSSIAN