ECOSSIAN - EUROPEAN CONTROL SYSTEM SECURITY INCIDENT ANALYSIS NETWORK

Newsletter

March 2017 - Issue 6

Ecossian

Message from the Coordinator

The ECOSSIAN project is in a very advanced stage. Being in M34, there are only two months left to finalize the project. During the past few months the main focus was put on the various national as well as the final European demonstrations. The first national demonstration was the Italian one on the financial sector, organized by *Poste Italiane* on 8th November 2016 in Rome. The second one was the Portuguese national demonstration which targeted the infrastructure sector, and was hosted by *Infraestruturas de Portugal SA* on 16th February 2017 in Lisbon. The Irish national demonstration organized by *Gas Networks Ireland* took place on 1st March 2017 in Cork and concerned the gas sector. At the moment efforts are bundled to prepare the final transnational demonstration, which will take place on 26th April 2017. This European demonstration will involve several partners and all SOC layers presented in the full technical solution. It will be performed in *Airbus Cybersecurity SAS* premises in Elancourt, near Paris.

In this Issue

Technical Meeting Elancourt, France

From 31st January—1st February 2017 , the ECOSSIAN consortium met for a technical face-2-face meeting in Elancourt, France. The meeting was hosted by partner *Airbus Cybersecurity SAS*. Besides discussions concerning the technical work for the upcoming months, the meeting was mainly dedicated to the demonstrations and the ECOSSIAN workshop that will be organized on 25th April in Paris. Before starting the preparation of the Portuguese (16th February), the Irish (1st March) National and the final European (26th April) demonstrations, a short wrap-up of the Italian National demonstration as well as the first Irish demonstration was provided by *Poste Italiane* and *Bord Gais*, respectively. This was followed by a technical workshop for the transnational demonstration organized by the demo lead *Airbus Cybersecurity SAS*. On the second day compliance issues with several requirements to the ECOSSIAN system were assessed and discussed. Another major focus of the second day was the ECOSSIAN workshop taking place in April. A draft agenda was created, possible key note speakers were proposed and promotional materials to be prepared were discussed.

Italian National Demonstration

The Italian Demonstration of the ECOSSIAN platform was held at Poste Italiane's premises in Rome on 8th November 2016. *Poste Italiane (PI)* is a national and international benchmark in postal, courier, logistics, finance, insurance, and, most recently, the mobile phone market segments. The demonstration consisted in a **simulated advanced and persistent threat (APT) attack** directed against PI. APTs are among the **most severe phenomena** in today's landscape of cybercrime. During the demo, attendees were asked to provide **feedback** on the ECOSSIAN platform and **solutions** according to the foreseen objectives of the project. Overall, the project received positive feedback. Participants proved particularly satisfied with some of the key goals the project aimed to achieve, such as the **integration of the ECOSSIAN platform with the national security strategy**, its ability to share **information in real time** with attribute-based encryption (ABE) technologies. On the other hand, constructive remarks focused on the possibility of integrating ECOSSIAN within their own organization, meaning that future efforts could be directed towards the **development of more marketable solutions.**

Italian Demonstration – the event was started by Ms. Alessandra Toma – Responsible for Information Security – and the Poste Italiane's team presenting the context and main challenges at the core of the ECOSSIAN project. Two screens have been used to simoultaneously display both the attack and the response given by the ECOSSIAN platform.

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:	Daniel Meister daniel.meister@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

March 2017 - Issue 6

Ecossian

Portuguese National Demonstration

The great visibility of any incident on railway infrastructure makes it an attractive target for many groups seeking for an immediate way to achieve visibility or a terrorist goal. As an operator *Infraestruturas de Portugal, SA (IP)*, which is the Portuguese National Railway and Road Administration Organisation, is committed not only to provide a service, but also **security functions** as well as measures for security supervision purpose. The Portuguese demonstration of the ECOSSIAN system took place on 16th February 2017 and resorted to a mix of simulated SCADA (not to disrupt operations) and real IT systems to demonstrate how the set of **solutions provided by ECOSSIAN could be used to detect and handle a complex advanced cyber attack**. More than 60 people from academia, critical infrastructures (CI) operators, military, regulator, law enforcement agencies, etc. attended the event.

Portuguese Demonstration at the headquarters of Infraestruturas de Portugal (IP) – simulated attacks to test the defence of IP, which manages the motorway networks, railways and has a telecommunications operator.

Irish National Demonstration

The overall goal of the demonstrations is to give a comprehensive demonstration and explanation of the capabilities of the integrated ECOSSIAN system deployed in operational contexts. The aim of the Irish demonstration was to show the detection of a **cyber-attack on a gas provider infrastructure**—*Gas Networks Ireland.* This demonstration is an accurate representation of how the SCADA network of Gas Networks Ireland reads and writes gas process telemetry data between its data centre, Grid Control and Above Ground Infrastructures (AGIs) around the country. The demo is based around information from AGIs being falsified causing Grid Control operators to make incorrect decisions and is a plausible representation of transmission gas networks. As for the attack, the hacker compromised the gas provider network through a **"man-in-the-middle" attack** on the telemetry readings. This type of attack enabled the attacker to secretly **relay** and then **alter the communication** between the SCADA servers and the AGIs who believe they were directly communicating with each other. The aim of the attacker was to induce the Grid Operator on the belief that there is a **massive gas leak** on the pipe. The Grid Operator would then **close the block valves**, thereby **isolating the town and electricity power station from the gas network.** 16 participants from a representative set of infrastructures, industry and academia attended the demonstration on 1st March 2017 in Cork, Ireland. Everything went smoothly and each step of the demo worked exactly as it should. Good feedback from the stakeholders regarding the project maturity and objectives was provided. Further interesting discussions evolved later on during the informal get-together.

Upcoming Events

IMPORTANT

- **ECOSSIAN Workshop**
  (affiliated to the EuroS&P)
  25th April 2017, Paris, France
- **Final European Demonstration**
  26th April 2017, Airbus Cybersecurity, Elancourt, France

Cooperation activities

During the last couple of weeks and months ECOSSIAN was engaged in several cooperation activities with other EU funded projects.
From 25th—27th January 2017 KU Leuven attended the Conference on Computers, Privacy & Data Protection in Brussels, Belgium. There they had a meeting with representatives from the **DOGANA project** in order to work on legal guidelines for human operators.
Another cooperation initiative was realized with the **CyberWISER project**. A conference call between representatives of the CyberWISER and ECOSSIAN project helped to discuss collaboration possibilities and how the two projects can benefit from each other's results.
A similar approach was followed with the **CIPSEC project**, in order to cooperatively promote each project's outcomes.

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: Daniel Meister
daniel.meister@airbus.com
Project Website: www.ecossian.eu

LinkedIn

FOLLOW US ON twitter

https://twitter.com/FP7_ECOSSIAN