PoSecCo
Policy and Security Configuration Management

For more information please visit our website
www.posecco.eu

Project title: Policy and Security Configuration Management (IP)
Start date: Oct 2010
Duration: 36 months
Total cost: Euro 11.3 M
Grant agreement no: 257129

Contact: Henrik Plate, henrik.plate@sap.com

PoSecCo is partially supported by the European Community under the Information and Communication Technologies (ICT) theme of the 7th Framework Programme for R&D (FP7).
Motivation
IT business service offerings are increasingly realized by the composition of in-house and outsourced subservices, partly for functional aspects, partly for infrastructure such as bandwidth or storage.

Service providers need to tackle a multitude of security requirements stemming from different sources, e.g., laws and regulations, customers, suppliers, or internal risk analysis.

- Is the current system landscape still in sync with the designed security concept, or did a change during operations jeopardize the security concept?
- How to improve the transparency for auditors, customers and service provider internal staff, and how to optimize audit activities?

Today, many of these challenges are addressed by manual, paper-based and as such labor-intensive, and error-prone processes. They may result in insecure and non-compliant systems and decrease profitability.

Objectives
The project aims at improving the security and compliance level of IT service providers, while lowering the costs caused by the management of security requirements, policies, and configurations.

Typical requirements demand the protection of cross-organizational communication channels or access control for all elements of the service landscape, starting from business services down to lower layers of system architectures. All of these requirements need to be met in a shared, partly outsourced and continuously changing environment.

Challenges faced by IT service providers are manifold, e.g.:
- Are the security requirements of new customers met by the current security concept and by current suppliers?
- What are the most efficient and cost-beneficial security controls to meet the requirements?

As such, PoSecCo aims to relieve the IT service provider of the burden to trade-off security and profitability goals, a prerequisite for the adoption of future, service-based applications which rely on a large number of provider-consumer relationships on all architectural layers.

Altogether, we aim at
- facilitating the analysis of security requirements, in order to understand and resolve potential conflicts;
- supporting the matching and comparison of 3rd party suppliers with regard to the relevant requirements;
- supporting security decisions related to the comparison, selection, and implementation of the “best” security control, based on their respective costs and benefits;
- overcoming sample based audits, by going towards a complete, repeatable, and automated validation and audit of security settings in a productive environment.

Key concepts
At the heart of the PoSecCo approach is the creation of a transparent, reliable, and sustainable link between security requirements on one side, and technical security configuration settings on the other side. Once this policy chain is established, and provided that it can be maintained throughout operations time, it becomes the basis for a large variety of applications that improve efficiency of policy and configuration management. This link will interconnect models of various kinds, starting with formalized requirements down to system models that describe the actual landscape and the IT services realized therein.

PoSecCo software is based on ITIL concepts, and supports policy and configuration management throughout various lifecycle phases of the service provider’s security concept:

At design time, security requirements from different sources are captured and analyzed. A decision support system analyzes the effectiveness of different security controls to meet these requirements, and proposes relevant alternatives to the decision maker, hereby considering costs as an additional criterion. Selected security controls are refined and result in the generation of low-level, technical security configurations that can be deployed in the landscape.

At runtime, changes of high-level security requirements are captured, and system landscape changes are detected in an automated fashion. The security and compliance impact of such changes is analyzed and assessed. The resolution of problems may be done in an automated fashion, e.g., by re-deployment of the golden configuration, or by human intervention in the course of ITIL processes for change and configuration management.