Policy-based Security Tools and Framework

POSITIF

Rigorous approach to increased protection

Open security framework

Simplified security management

Easy integration of heterogeneous security technologies

POSITIF

Information Society Technologies

www.positif.org

Project structure

POSITIF is an international research project funded by European Commission under the Sixth Framework Programme.

The main goal of the project is to offer automatic tools to support security managers in protecting networked infrastructures and applications. The ideas and solutions developed by POSITIF will be available as open-source and commercial products.

POSITIF uses a formal approach to describe the system to be protected, the security policy to be enforced and the security capabilities available. A set of tools is offered to verify the policy's coherence, create the proper configuration of the security elements, automatically deploy it and periodically monitor its correct enforcement

The project consortium includes research institutes, end-user representatives and industrial companies that work together towards making the vision of POSITIF come true.

Target groups

Scientific sector - researchers in the fields of ICT security, system management and monitoring

Security-related companies - developers of security products (especially SMEs with niche products) and security consultants

Non security-related companies - system and security managers, ICT auditors, IT decision-makers

European Commission - policy makers in the fields of ICT security and open-source software

Benefits of the project

Scientific sector

New results in the fields of system modelling, security analysis and system management.

This includes languages for system and policy description, policy refinement strategies, security measure techniques and data analysis strategies towards anomaly identification.

Non - security related companies

Ability to use a single security management system across different technologies and producers.

Tools to measure the achieved security level and perform what-if analysis.

Innovative approach to intrusion detection and system operation monitoring for better auditing capabilities.

Security - related companies

An open-source framework for security management, with hooks to integrate different tools and technologies. This would greatly benefit the producers of niche security solutions that could exploit other parts of the POSITIF framework such as automatic configuration, deployment and monitoring.

Moreover the provision of formal rigorous tools for system description and security analysis would support the work of external security consultants by providing a baseline analysis of the target system.

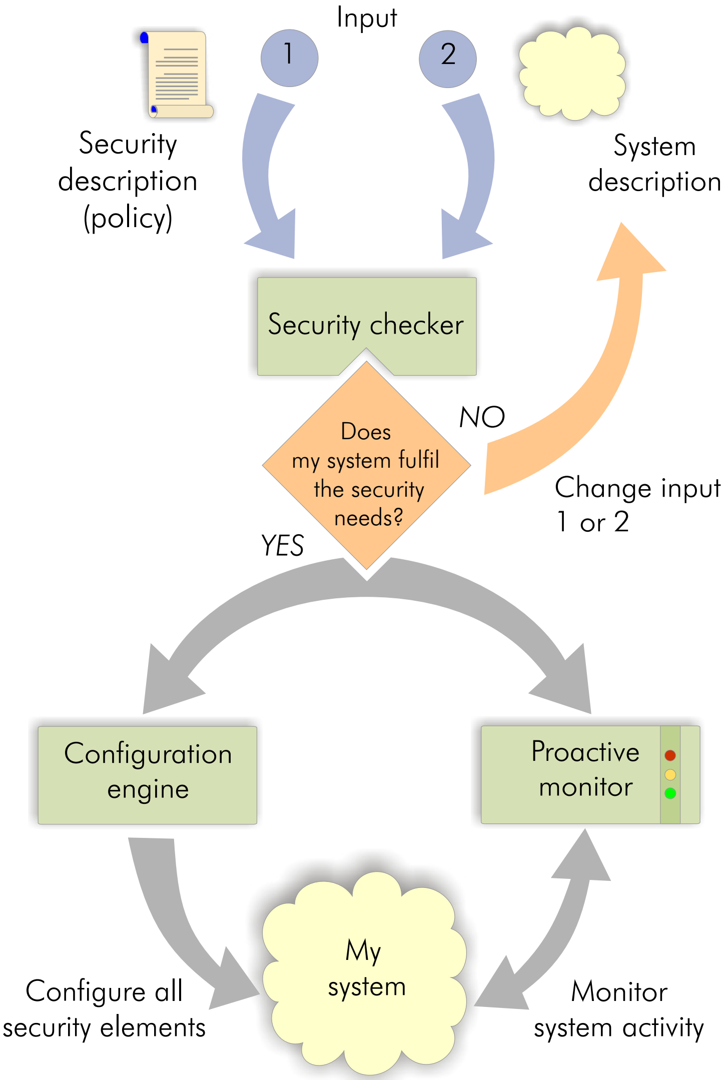
European Commission

Contribution to European Union policies by providing hooks for integration of SMEs work and creation of security solutions based on open-source software and global standards

What you get

The framework is activated by providing two descriptions: the required policy and the managed system. The idea is to describe the security requirements along with the topology and functionality of the target networked system, including the available security capabilities of each node.

For generality and compatibility with other tools, the POSITIF framework uses CIM (the Common Information Model) for system and policy description and exchanges data based on XML formats.



Security checker

The interesting question for every system administrator is: will my system fulfil my security needs ?

POSITIF offers a module - the security checker - to answer this question accurately. Additionally, this module produces a measurement of the actual protection level achieved by the chosen policy on the given architecture.

Configuration engine

After checking that the system is able to satisfy the security requirements, the administrator must properly configure all the nodes. When thinking of a multi-vendor and/or multi-hw/sw platform, this is not an easy task.

The POSITIF framework supports this activity via an automatic configuration engine to translate the generic policy into real device (or application) configurations and upload them to the various protection elements (e.g. firewalls, routers or applications with proper access control mechanisms).

Proactive security monitor

The proactive security monitor performs network and nodes surveillance, looking for any behaviour that violates the deployed security policy. It collects events through sensors and compares monitoring data against a set of known attacks and the security policy.

This method allows the detection of unknown attacks as policy violations.

Additionally, automatic or semi-automatic reaction can be requested. If a security violation is detected an updated security policy can be deployed to the whole or part of the target system. The monitor also tests the proper application of the enforced policy by sending dummy attacks and verifying their detection.

Examples of usage

POSITIF will be tested in three typical environments that have different security requirements:

- a high-speed academic network (that of the Wroclaw University of Technology) where security is important but it must not interfere too much with the research and teaching activities
- the Intranet of a large governmental organization (that of the Ministry of Justice in Italy) that requires a high level of security
- the back-end network of a mobile phone operator (Vodafone) where business continuity is of utmost importance

Contact

Project Coordinator

Prof. Antonio Lioy

Politecnico di Torino
Corso Duca degli Abruzzi, 24
Dip. Automatica e Informatica
10129 Torino,Italy

Tel: +39-011-5647021
Fax: +39-011-5647099
Email: lioy@polito.it

More information

Project website: http://www.positif.org
General contact address: info@positif.org

Project partners

Politecnico di Torino
Italy

BearingPoint
INFONOVA GmbH
Austria

Bull SA
France

Ministero della Giustizia
Italy

PRESECURE
Consulting GmbH
Germany

Wroclaw University
of Technology, WCSS
Poland

Stiftung Secure Information and
Communication Technologies
Austria

Saint Petersburg Institute
for Informatics
and Automation of the Russian
Academy of Sciences
Russian Federation

Universidad de Murcia
Spain

Vodafone Omnitel N.V.
Italy