INNOVATION REPORT 10035 PREDYKOT Thierry Winter, Evidian SA, France

PREDYKOT

Intelligent security and smart access control for online networks

With 'the cloud' increasingly hosting more and more computing tasks and data, online security, authorisation and identification have become vital, especially in markets where security is crucial, such as banking, cloud computing, mission-critical systems, network access and professional mobile radio systems. This growing dependence on online access is coupled with variety and sophistication in the threats that endanger that access. PREDYKOT set out to radically rethink approaches to security to enable organisations to develop security strategies and software to respond dynamically to organisational changes and reconfigure themselves to adapt to new conditions, thereby introducing intelligence into security governance and closing the security policy loop.

Smart reasoning

This ITEA 2 project shifted the focus of the management of the security policy from automation to a more intelligence-based approach, using critical intelligence to constantly update the security policy and consequently further improve business processes. The intelligent mechanisms developed in the project ensure that security policy not only becomes and stays efficient but also incorporates contextual information to enable the policy to be dynamically refined on a continuous basis. The new policy and reasoning languages developed by PREDYKOT combined the best of different policy-specification languages, events from management policies and authority from security policies on the basis of existing standards such as the extensible access control mark-up language, XACML, thereby enabling the specification and interpretation of security policy to be simplified. Tools were used to analyse the security policies specified by this language and to detect, for example, possible conflicts or inconsistencies in the policy specification.

A suite of modules

The software suite of models PREDYKOT created will dynamically improve security policy and keep it on track, using:

- reasoning engines on user activities, policy changes and contextual information;
- smart nodes as actuators or sensors for the information system;
- interfaces with security-information and event-management systems;
- fusion of distributed data and data management;
- workflow and security portal for feedback on the policy; and
- steering dashboard.

In smart nodes, for example, a semantic approach enables intelligent agents to exploit technologies so that the nodes can sense their environment and share knowledge, providing adaptive mechanisms to adjust the policy as the world changes and as new information becomes available. Anticipating the massive deployment of smart nodes in environments like personal mobile devices, PREDYKOT developed smart nodes that are able to calculate metrics, adapt policies and provide in-depth accurate information to specialised reasoning engines.

New product for security intelligence market

The diversification of and continuous changes in digital risks encountered by any organisation make security policy management an increasingly complex task. The highly innovative complete and coherent ecosystem of security-policy modules along with an application methodology developed in the PREDYKOT project can be considered a brand new product for the security intelligence market: a unique eco-system of interoperable, exchangeable modules. This software suite will continuously adapt security policies to changes in the risks inherent in administration, user activities or context, reacting to reports to modify the policy in real-time.
In addition, the methodology guidelines – ranging from policy design methodology to the everyday steering of the policy using metrics for governance, risk management and compliance – will help deploy the PREDYKOT ecosystem in a realistic and pragmatic manner.









Evaluating and extending security management standards

The project partners used case studies to evaluate existing security management standards, or propose extensions to those standards, in the domains of semantic representation of a policy, security metrics, policy deployment methodology such as ISO 27001 or EBIOS, and reasoning languages. PREDYKOT also worked in close cooperation with the ITEA 2 EASI-CLOUDS project, which is developing a new cloud-computing infrastructure based on European and open standards, using the EASI-CLOUDS environment to test a number of key security policy capabilities, and thus prove the effectiveness of its approach. Indeed, other newer ITEA projects are already using some of the results of the PREDYKOT project: ADAX (contextual reasoning), Web of Objects (reasoning engine).

The project managed to book progress in the area of standardisation where collaboration took place with several ISO/IEC standardisation bodies. For example, the Finnish consortium partners worked with ISO/IEC 27000 series and IEC standards through FISMA and SESKO, and contributed to the revision of the ISO 27000 series standards while Thales presented the PREDYKOT principles to the French Standardisation Office for the standardisation of aeronautics and space along with proposed improvements to OASIS for the XACML 3 standard. Further to this, collaboration occurred on the editing of manuals relating to cyber-security of industrial systems at ANSSI and Cassidian averaged one presentation per week related to PREDYKOT technologies to customers in response to requests from customers to take into account reasoning engines.

There were three demonstrations: Professional Mobile Radio (PMR), Smart Grid, Identity and Access Management (IAM). The PMR demonstrator concerned malware through the USB key and was illustrated via virtual machines. The Smart Grid demonstrator focused on video and access rights policy including single sign-in on multiple devices and the IAM demonstrator explored three banking use cases in a running demo.

Real-life deployment of PREDYKOT results was made possible thanks to standards and abstraction layers, e.g. common representation of policies (XACML v3) and scalability was provided by the data fusion engine while adaptable workflow allowed a mix of automatic and manual reasoning. The reasoning rules have now been fully implemented and can handle policy, event conflicts and the like.

Demand-driven exploitation

On the exploitation front, there has been reported strong demand from customers and the consortium partners lost no time in responding. In early 2015, Evidian plans to release a new option of Access Intelligence in the next version of its Identity and Access Management product. This same year, Cassidian expects to provide a full decision-support solution in the Security Management area with a call for tenders in the Middle East and requests in Sweden, France and the Netherlands. Gemalto also anticipates the completion of technologies for Trusted Service Manager products in 2015. Thales is convinced that the developments generated in the PREDYKOT project will be beneficial to crisis management solutions, cloud IAM solutions and XACML developments (optimisation, cloud) while a commercial alliance between ZIV and Nextel will focus on making smart grid operation cheaper, targeting international markets (Mexico, US). SMEs have also benefited from the developments and results of the project as they look to enhance their product portfolios.

By improved compliance and security, and fostering ethics through compliance, the PREDYKOT project has responded to a real industrial and societal need, one that will only become increasingly critical as all kinds of markets, from banking to networks, are faced with a growing dependence on online access and all the concurrent dangers this poses. By creating a unique eco-system of interoperable, exchangeable modules, organisations are able to develop security strategies and software that are able to respond intelligently and dynamically, adapting to new conditions, and so benefit from intelligent security and smart access control for online networks.

More information:
www.itea2-predykot.org