MULTIPOL
(ITEA 2 07001)

Thierry Winter, Evidian
France

Securing access across multiple domains

The ITEA 2 MULTIPOL project has developed an innovative modular and consistent security suite enabling fully automated runtime access between independently administered domains with the implementation of strong security features. This is based on coherent authorisation mechanisms which take into account the different security policies enforced in the individual domains. The results of the project were demonstrated in a healthcare application speeding secure access to patient files between different hospitals.

Flexible yet robust identification and authorisation – be it radio-frequency identification (RFID), biometry or strong authentication with digital certificates – is essential for commercial and research organisations that increasingly work with external groups and consortia. The demand is to extend business and other processes outside normal boundaries to enable electronic exchanges with partners and suppliers.

Even within an enterprise, different business units often manage distinct sets of users and resources. The deployment of service-oriented architectures (SOAs) or the composition of Web Services pose similar problems: the different services can relate to different companies or organisations, with different policies for enforcing the security of each service.

IMPROVING AUTHORISATION IN MULTI-DOMAIN ENVIRONMENTS

Authentication and authorisation are the key elements of security mechanisms for access control. While much has been achieved in the area of authentication, authorisation has not been properly standardised nor even sufficiently understood in multi-domain environments, where all domains are administered independently and are enforcing different security policies.

No single company is able to handle the external inter-domain processes end to end by itself. Such inter-organisation security requires co-operation with inter-domain access control – the type of approach developed in MULTIPOL. This ITEA 2 project set out to specify and implement a complete authorisation chain, applicable to multi-domain environments. In addition to mechanisms applied at runtime, such as converting profile roles and attributes, or negotiating and reacting to a contextual security level, MULTIPOL has implemented out-of-band mechanisms, aiming at comparing security policies for compatibility, intelligent composition, etc.

MULTIPOL focused on three principal problems:

1. Securing the expansion of business processes beyond the usual organisation boundaries;
2. Providing the essential security policy mechanisms to enforce access control; and
3. Controlling the access to applications and information across security domains.

Key advances included:

- *A multi-purpose authorisation chain* which required the development of a technical chain of modules to ensure authorisation for access control, including a Policy Administration Point, a Policy Decision Point and Policy Enforcement Points;
- *Security policy composition* – if a company wants to be a member of a consortium, secured by MULTIPOL, its domain has to be compatible with the set of security rules given by the consortium. A company can continue to use its own rules internally but now has additional rules selected pragmatically to enable it to work with the consortium – this involves 'composition' of local company policy and global consortium polices to enable work with the consortium; and
- *A suite of tools and software components* addressing the design, implementation, deployment and management of a comprehensive security infrastructure assuring a consistent security policy in multi-domain environments.

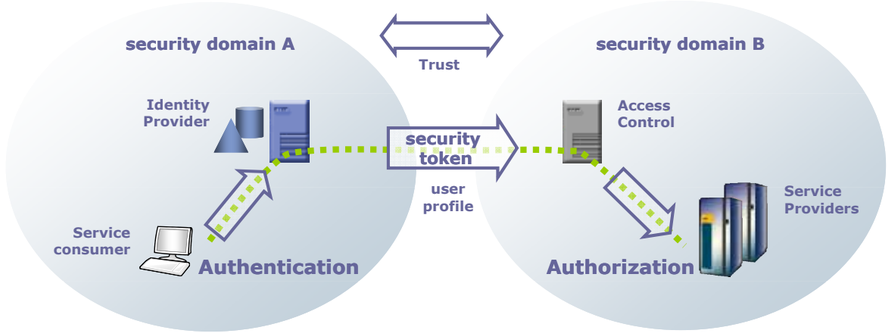
RECONCILING SEMANTIC DIFFERENCES

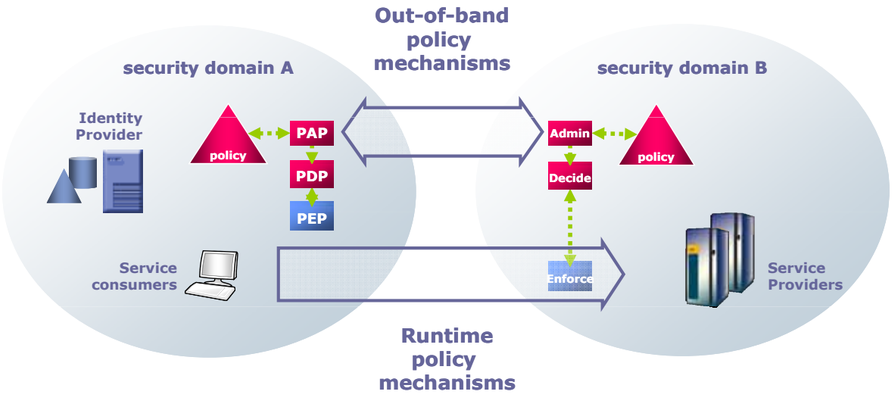
Authorisation in multi-domain environments can be established by integrating the access control policies of collaborating domains. MULTIPOL took a more realistic approach by composing each local existing policy with a set of rules, global to the consortium of domains. The resulting composed policy is enforced by each domain at runtime, when users or services access to resources.

Existing methods for expressing access control policies offered restricted extensibility and lack of semantic expressiveness, interoperability and reasoning capabilities. MULTIPOL circumvented this critical limitation using an ontological approach that offers a new abstract ontology on top of the proposed policy representations: XACML and extended RBAC.

Important advantages resulting from the use of MULTIPOL software include:

- Maintaining the local security policy while enforcing extra policy rules for the multi-domain co-operation;
- Abstracting the security implementation using a semantic approach; and
- Helping map to real-life deployments with a modular suite of components.





Two markets were selected for demonstration of the MULTIPOL approach.

1. *The healthcare sector* – the major effort was focused on simplifying secure inter-hospital access to patient records. While a doctor established in a hospital will have access to in-house records controlled by local access rules, access to the file of a patient from another hospital is more complicated. Currently, it is necessary to phone the other hospital, explain what is wanted and request access. MULTIPOL provides automatic access to the second hospital as part of an inter-hospital consortium; and
2. *Interbuilding access* – this more limited demonstration involved sharing of information between highly secure buildings such as embassies. This was designed to allow access to applications and databases between embassies.

QUICK EXPLOITATION OF RESULTS

Enterprise security and inter-domain security are key topics globally in a market with currently strong competitors in the USA. MULTIPOL brought together French and Spanish researchers working on access management and control, and systems integrators building such systems. European-level co-operation was seen as essential to provide all the skills necessary.

The project was deliberately short to enable a quick exploitation of results. Project leader Evidian has already included some modules developed in MULTIPOL in its standard product offer – such as in its latest identity and access-management software suite launched in September 2010.

Other partners have plans to integrate results during 2011.

Success in the ITEA 2 project has also helped increase the visibility of the European software industry in this area of security. It enabled consortium members to communicate their success to the key industry analysts that influence their customers by demonstrating that European companies are spending money on multi-domain security.

Standardisation did focus on sending recommendations back to the OASIS standardisation body, to show how use was being made of existing international and US-driven standards and to outline areas where such standards should be improved.

More information: www.itea2-multipol.org