Integrated Management of Security Policies

Stefano Paraboschi

Integrated Management of Security Policies

Stefano Paraboschi

Universitá degli Studi di Bergamo, Italy, parabosc@unibg.it

Abstract. The design of an integrated approach for security management represents a difficult challenge, but the requirements of modern information systems make extremely urgent to dedicate research efforts in this direction. Three perspectives for integration can be identified.

1 Challenges to Security Policy Management

The management of security policies is well known to be a hard problem. Significant attention has been paid in the past to the design of flexible and powerful solutions for the high-level representation of a security policy and its translation to a concrete configuration, but the impact on real systems has been limited. Indeed, most information systems today present an extremely partial support of security policies. Network security is typically the portion of the security domain that exhibits the greater support by tools, with the possibility to define high-level requirements and to get support on mapping them to concrete configuration. The other components of the system are instead managed with labor intensive processes. When automation is used, it relies on configuration scripts and ad hoc solutions. In general, the security policy is documented at the lowest level, as a concrete set of configurations of devices and system modules.

The analysis of long-term trends in the evolution of the ICT scenario makes very clear that the importance and complexity of security policy management is going to increase. Information systems are becoming more extensive, integrate resources of different owners, and offer access to a larger variety of users. Service oriented architectures are an instance of these trends, supporting the realization of large systems that implement functions with the integration of a variety of services executing under the responsibility of potentially independent providers. In addition, modern systems have often to demonstrate compliance with regulations to other parties. For instance, HIPAA, PCI-DSS, and Sarbanes-Oxley Act are leading in their specific domain to an urgent need for better security management solutions.

2 Conceptual, Vertical, and Horizontal Integration

A crucial aspect to consider for the evolution of security management is the need to offer a better integration in the management of security policies. The configuration of the concrete security policy of a specific system in isolation is not trivial, but it is not the main obstacle, since it can benefit from sophisticated

access control models that have been developed for a variety of systems, from relational database management systems to application servers. The significant obstacles emerge when the need arises to integrate and harmonize the security policies specified in different systems at different levels. Three clear integration perspectives can be identified:

- *Conceptual integration*: security policies have to be described at different levels of abstraction, from the business level to the concrete configuration of modules and devices. Separate models are required for the different levels, as testified by software engineering practice in many areas. Also, some support for translating the policy at a high level to a more concrete policy has to be provided. Describing the correspondence between the policies at different levels, compliance of the concrete policy with the high-level security requirements can be verified in a more effective and efficient way. In addition, a structure with different abstraction levels greatly facilitates the maintenance of the security policy.
- *Vertical integration*: the structure of a modern information system presents several components that can be represented in a vertical stack: physical hardware, virtual hardware, operating system, network, DBMS, application server, application. Security policies can be supported at each of these layers. The security policies at the different layers are typically defined independently, but a clear opportunity exists for their integration. The advantage of a careful integration is both a greater level of security and a greater level of flexibility.
- *Horizontal integration*: Compared to the classical scenarios considered in access control, where a policy is assumed to be enforced by a specific reference monitor, modern information systems present a variety of computational devices cooperating in the execution of a specific user request. The computational infrastructure can be owned by independent parties. In these scenarios, the management of security policies requires to carefully define models and mechanisms able to map a security requirement to a coordinated policy enforced by the different parties. This aspect is particularly difficult when few hypotheses can be made about the specific security management functionality supported by the service providers.

The PoSecCo project [1] plans to investigate these three aspects. Conceptual integration will rely on the design of metamodels structured at three levels: Business, IT, and Landscape. Vertical integration will specifically consider the harmonization between access control and network configuration. Horizontal integration will be considered in a Future Internet scenario, where applications are realized integrating the services of a variety of providers. A shared motif will be the detection and resolution of conflicts in the policies.

References

[1] PoSecCo, Integrated Project funded by the European Commission, FP7 Call 5, October 2010-September 2013, http://www.posecco.eu.