Identity and Access Control – Demonstrating Compliance

Marc Sel · Bart Van Rompay
PricewaterhouseCoopers
{marc.sel | bart.van.rompay}@pwc.be

Abstract
Identity and particularly access control present various challenges, particularly for larger organisations. The combined complexity of users from various communities, accessing multiple systems and applications in the context of business processes can be significant. The US NIST proposed the Role-Based Access Control model in order to effectively and efficiently manage authorisations. While this model certainly also has its drawbacks, it gave rise to various interesting software solutions. One particularly relevant one is the Sage tool. This tool builds a model of the actual authorisations across platforms by consolidating and enriching them in its own database. Subsequently, the built-in pattern-matching engine can identify a number of less desirable patterns in the data and can recommend solutions, e.g., for role structuring (role-mining). Furthermore, business constraints can be expressed in so-called business process rules, which can, e.g., reflect segregation of duty requirements.

In the pilot project described here as case study, we combined both role-mining and compliance verification. The case study organisation is subject to both national competition regulation and the US Sarbanes-Oxley act. They employ approximately 25,000 employees. Analysing existing access controls through a unified approach and applying compliance rules to them has shown to be a quick and reliable way for them to demonstrate compliance (or identify actions where compliance was not yet achieved). The fact that the control library is available both at the level of principles and at the level of specific business process rules makes the approach transparent, repeatable and affordable. Furthermore a number of observations were made that allowed to remove undesired authorisations through data cleaning. As a result of the pilot project the client decided to implement BPR-based compliance verification for all applications that are subject to Sarbanes-Oxley.

1 The challenge of Identity and Access Control

1.1 Introduction
Most medium to large sized organisations today built up and manage what could be referred to as their ‘authorisation space’. This space is essentially structured into three dimensions: the different user communities (subjects), the ICT services and applications (objects), and the processes allocating users authorisations onto these services.

This can be represented as:
The user dimension (subjects) is structured into various types of user communities, ranging from employees to partners and customers, or the public at large. Nowadays, even some regulators are asking access, or are forcing companies to open systems to competitors in order to liberalise a particular market. The services dimension (objects, left-to-right axis) can be further decomposed into individual applications or transactions within these applications. Finally, the authorisation management dimension (vertical axis) is organised into sets of processes that support the user authorisation life-cycle ("from hiring to firing/retirement").

In the real-world, this space can be impressively large. For one particular company with 40,000 employees (and excluding the authorisations of customers on company systems) we estimated the total number of authorisations that were managed around 35 million. Since that organisation’s authorisations were decided by a core team of 10 persons, this meant that on average, every authorisation manager was dealing with approximately 3.5 million authorisations. Most of these authorisations have been built up over the years, often surviving multiple rounds of business reorganisation.

1.2 IdM initiatives often fall short of meeting expectations

Many vendors tout Identity Management (IdM) systems as the overarching solution to the management of user identification and authorisation. Such systems are aiming essentially at quicker turnaround time for user-id and authorisation provisioning. These systems typically address the aspects of authentication, directories, provisioning and access control. While the actual success rate of such Identity Management projects varies, their approach with regard to access control is typically incomplete. High-level or coarse-grained access control can be managed, but more fine-grained or application-specific access control is often not addressed. Also, while web-based solutions are typically covered, legacy systems are often left out. For many organisations legacy systems will stay around for the near or not-so-near future.