Chapter 6.11
A Model-Based Privacy Compliance Checker[1]

Siani Pearson
Hewlett Packard Research Labs, UK

Damien Allison
Hewlett Packard Research Labs, UK

ABSTRACT

Increasingly, e-business organisations are coming under pressure to be compliant to a range of privacy legislation, policies and best practice. There is a clear need for high-level management and administrators to be able to assess in a dynamic, customisable way the degree to which their enterprise complies with these. We outline a solution to this problem in the form of a model-driven automated privacy process analysis and configuration checking system. This system models privacy compliance constraints, automates the assessment of the extent to which a particular computing environment is compliant and generates dashboard-style reports that highlight policy failures. We have developed a prototype that provides this functionality in the context of governance audit; this includes the development of software agents to gather information on-the-fly regarding selected privacy enhancing technologies and other aspects of enterprise system configuration. This approach may also be tailored to enhance the assurance provided by existing governance tools.

INTRODUCTION

In order to conduct business, organizations must try to assess and ensure compliance with privacy legislation, policies and regulations, as part of their IT governance initiatives. Such privacy management is an important issue for e-business organizations since e-business can be defined as "the utilization of information and communications technologies (ICT) in support of all the activities of business" (Wikipedia, 2008). This issue involves both operational aspects, related to the enforcement of privacy policies, and compliance aspects related to checking for compliance of these

DOI: 10.4018/978-1-61350-323-2.ch6.11

policies to expected business processes and their deployment into the enterprise IT infrastructures.

The Need for Automation

We address the problem of how to make privacy management more effective by introducing more technology and automation into the operation of privacy in e-business organizations. Enterprises are coming under increasing pressure to improve privacy management, both to satisfy customers and to comply with external regulation (Laurant, 2003) or internal policies. Not only are human processes prone to failure but the scale of the problem highlights the desire for additional technology to be part of the solution. The trend towards complexity and dynamism in system configurations heightens this need for automation to ensure that privacy and security properties are maintained as changes occur, and in addition to check that the privacy enhancing technologies are operating as desired.

Automated Compliance Checking Requirements

Most of the technical work done in this space focuses on the provision of auditing and reporting solutions that analyse logged events and check them against privacy policies and process guidelines. These auditing systems usually operate at a low level of abstraction and do not take into account the overall compliance management process that involves both the refinement of privacy laws and guidelines within enterprise contexts, their mapping into the enterprise IT infrastructure and their subsequent checking against the enterprise's operational behaviour.

At present there is a gap between the definition of high-level regulations, standards and best practices and what is actually happening in an enterprise at the level of application software, system software and middleware, processors, networks and data stores. The current approach is to fill this gap using people-based processes, but there are drawbacks to this, in terms of being slow, expensive, error-prone and leading to best-effort compliance due to limited resources. Our vision is to bridge this gap where possible with model-based technology and automation, as shown in Figure 1. On the one hand privacy policy enforcement technologies can be used to deliver compliance to privacy principles and goals; on the other hand (the focus of this article) we can use system monitoring technologies to continuously assess their actual performance and ability to deliver against the requirements of the policy.

Our Approach

To address this problem we are developing a Policy Compliance Checking System. Key requirements of this system are to:

R1. model privacy policies (based on company privacy policies, laws and guidelines or best practice). A mechanism is needed that enables such models to be defined and viewed. Predefined models should also be usable, and amendable by expert users if desired.
R2. map these models at the IT level. It is necessary to configure the models to the deployed system.
R3. analyze related events. The compliance checking system needs to monitor those properties of the deployed system that can affect satisfaction of the privacy policies.
R4. generate meaningful reports highlighting compliance aspects and violations. These reports should be understandable to non-experts, and allow drilling down to a greater level of detail.

This system should supervise and report on the availability of other privacy enhancing technologies (PETs) – for example, privacy policy enforcement systems, obligation management systems and security technologies – and check for