Chapter 10
Privacy Compliance Checking using a Model-Based Approach

Siani Pearson
Hewlett Packard Research Labs, UK

Damien Allison
Imagini Europe Limited, UK

ABSTRACT

Organisations are under pressure to be compliant to a range of privacy legislation, policies and best practice. At the same time many firms are using privacy as a key differentiator. 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, and to provide increased feedback to end users about the degree of privacy and security compliance that service providers are actually providing.

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. As well as these 'data protection' concerns, there may be an intangible value in proposing an 'open' approach to privacy compliance, for example by showing all privacy-relevant information as is done within the Google dashboard (Google, 2009). Such privacy management is an important issue for e-business organizations since e-business can be defined as "the utilization of information and communica-

DOI: 10.4018/978-1-60960-132-4.ch010

tions technologies (ICT) in support of all the activities of business" (Wikipedia, 2010). This issue involves both operational aspects, related to the enforcement of privacy policies, and compliance aspects related to checking for compliance of these policies to expected business processes and their deployment into the enterprise IT infrastructures. A 'web of trust' may also be involved in order to determine when to share personal and sensitive information: for example, credit card details.

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. An alternative approach is to rely on the users 'voting with their feet', in the sense of using a company that they trust because they are familiar with it, but nevertheless this company still needs to be legally compliant. 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 (including 'always on' controls).

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. 'Unit level' business model invariant solutions such as (Goossenaerts, 2009) rely on this type of approach without modelling higher level dependencies on low level issues.

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 generally 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 chapter) we can use system monitoring technologies to continuously assess their actual performance and ability to deliver against the requirements of the policy. The key to this approach is to capture the tacit relations between low level signals and indicators and high level goals.

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.