Chapter X

Modeling Method for Assessing Privacy Technologies

Michael Weiss, Carleton University, Canada

Babak Esfandiari, Carleton University, Canada

Abstract

In this chapter we propose a modeling framework for assessing privacy technologies. The main contribution of the framework is that it allows us to model aspects of privacy and related system concerns (such as security and scalability) in a more comprehensive manner than the dataflow diagrams traditionally used for privacy analysis. The feature interaction perspective taken in the chapter allows us to reason about conflicts between a service user’s model of how the service works and its actual implementation. In our modeling framework such conflicts can be modeled in terms of goal conflicts and service deployment. Goal conflicts allow us to reflect conflicting points of view on system concerns (primarily privacy and security) among the different stakeholders, which are part of the system and its context. Deployment refers to the assignment of functionality to system components, which allows us to reason about dataflows between components, as well as potential conflicts of interest. As a demonstration of the framework, we illustrate how it can be applied to the analysis of single sign-on solutions such as .Net Passport.
Introduction

Late in 2004, Rice University researchers uncovered a flaw in Google’s Desktop Search tool that could release private local data to an untrusted third party. Earlier in 2004, a flaw in Apple’s Safari Web browser was reported that allowed an attacker to upload and execute an arbitrary program on the user’s machine. These flaws spotlight some of the security and privacy risks users are exposed to when systems are composed from independently created components or services that interact in unexpected ways.

In both examples, the application designers had made incorrect assumptions about the identity of the initiators of service requests. For example, in the case of the Safari Web browser flaw, the help viewer would execute scripts referenced in an URL and not check who made the request. It was assumed that it would originate with the help viewer. This “feature” of the help viewer could be exploited by downloading and mounting a disk image with a malicious script and then asking the help viewer to execute it.

Such unexpected interactions are also known as feature interactions. Feature interactions occur when independently developed and separately tested components (also known as features) are combined, and the combination results in undesirable side effects. They are difficult to anticipate, in particular in an open system such as the Internet, due to the combinatorial number of ways features can interact with one another. These side effects are often non-functional in nature and in many cases are related to privacy or security.

As the examples show, failing to consider the actual identity of the requestor of a service may cause serious privacy and security breaches. The authenticity of a user or service provider on the Internet cannot be taken for granted. A variety of techniques — smart cards, personal information devices, single sign-on services, to name but a few — have been developed to address this issue. However, the benefits and convenience of these techniques must be weighed against the privacy and security issues their use may raise. The focus of this chapter is, thus, on privacy technologies and assessing them for privacy issues. For these to be accepted in the user community, we must ensure that there are no new privacy and security risks by using the very techniques intended to address such issues. We introduce a modeling framework for assessing privacy technologies and their possible side effects on overall system concerns such as privacy and security, and demonstrate its use for analyzing the privacy pitfalls of single sign-on services.

Privacy Assessment

Privacy concerns the collection, storage, use, and sharing of data about individuals (Cannon, 2005). It has several dimensions, including the protection of personal data, or privacy protection. Individuals do not want data about themselves to be shared with other parties without their consent, and when data is held by another party, they want to have control over the data that is held about them and its use (IPC, 2000).