Privacy Systems

Carl A. Gunter
University of Pennsylvania

Michael J. May
University of Pennsylvania

Stuart Stubblebine
Stubblebine Research Labs

January 2004

Abstract

The world of wireless services has become richer and more diverse at a rapid pace. What one were tools available only to large commercial enterprises and the military have become available for mass market use. With that shift consumers have acquired an appetite for ready-made personalized services that fit their immediate needs and convenience. The problem with that explosion is that not enough analysis has been done to ensure the privacy of the consumer, providing real assurance about how collected data is used and modified by the service providers.

In order to discuss and concretize permissions on user data it is helpful to rely on digital contracts - signed digital documents that describe rights that one principal may exercise on the data of another. To reason about how permissions on data are managed, created, and interpreted, we describe a formalism called a Privacy System. A Privacy System is a formal model of the principals, data, and digital contracts needed to give specific assurances of the integrity and privacy of personal data. We describe the interactions between different principals to see how protected data can and should flow.

Using the model of a Privacy System it is straightforward to create an implementation that respects its rules. Since the system is based on a well described formal model, we have assurance that the pieces will work as specified. Additionally, since the model abstracts away particular implementation details, it would not be hard to make clients that can interact properly with any particular implementation of a privacy system.

As a case study, we consider the particular task of protecting location information that is given to certain information subscribers to provide a desired service.

As part of the above mentioned digital contracts, we have created a language that allows computer understandable privacy policy formats. The W3C's P3P privacy policy language is used to describe permissions and rights that may be exercised in the context of a digital contract. For a contract language we choose ContentGuard, Inc.'s eXtensible rights Management Language (XrML), an extensible contract language useful for expressing unambiguous digital contracts. By combining P3P and XrML into a privacy policy contract language we replace long, hard to interpret privacy policies with computer understandable policies that can easily be compared to each other.

The combination of understandable digital contracts and systems that conform to models that respect privacy has ramifications in many areas. Our case study in geographic location based services is one example. Others applications include systems that enforce HIPPA regulations, systems for managing private patient data used for medical studies, and systems for credit card companies to track and detect fraud, all of which can be shown to respect the privacy of the data being managed.