A Comparison of Two Architectures for Implementing Security and Privacy in Cyberspace

Reind van de Riet\textsuperscript{1}, Wouter Janssen\textsuperscript{2}, Martin Olivier\textsuperscript{3}, and Radu Serban\textsuperscript{1}

\textsuperscript{1} Department of Mathematics and Computer Science
Vrije Universiteit, Amsterdam
\{vdriet,serbanr\}@cs.vu.nl
\textsuperscript{2} ERS-Deloitte\&Touche, Amsterdam
wojanssen@deloitte.nl
\textsuperscript{3} Department of Computer Science
Rand Afrikaans University
Johannesburg, South Africa
molivier@rkw.rau.ac.za

Abstract. In this paper we compare two approaches for implementing Security and Privacy systems in Cyberspace: a structured approach, such as done in Mokum, where access is governed by structure (of the classes), and two principles: the epistemic and the ontologic principle. The second approach is based on the use of capabilities, such as provided by ERP systems. Keywords: security and privacy, cyberspace, architecture, object-orientation, capability.

1 Introduction

Information about individuals is stored in many places which has led to the so-called privacy problem. In technical terms this means that access to this type of data is governed by specific rules specifying who is allowed/obliged to do what on this data under which circumstances. We will call these rules privacy rules.

When more than one company is involved in data about an individual, say a hospital H, and an insurance company IC, they may use Internet to communicate with each other using a secure connection based on crypto-techniques. Actually, there are actors in H and IC, represented by certain (software) agents whose functioning is prescribed in Work Flows (WF). The privacy rules will now directly refer to these WF's as they describe the circumstances in which the individual's information is needed. In another paper we will deal with the interaction of privacy rules and WF [TR2000]. In the current paper we will concentrate on two quite different architectures which must provide a trustworthy and flexible security systems. These architectures are: the ERP architecture, based on capabilities, and the Mokum architecture, based on structure.

The Mokum architecture has been developed in our group already some ten years ago. It is an object-oriented system where the objects are active sending
each other messages and receiving answers. This is optimally suited to be repre-
sent by agents. To maintain privacy rules special objects can be created called
keepers whose main task it is to maintain the integrity and Security&Privacy
(S&P) rules for collections of objects. Using the static structure of the objects
and special properties of these keepers it is possible to specify systems which are
provably correct with respect to the privacy rules. This is based on two prin-
ciples: the epistemic principle, which is implemented by reasoning features in the
Mokum compiler and the ontologic principle which is provided by the Mokum
run time system and checks the relationships between a caller and a callee. In
[RB94] we have shown the universal applicability of these principles. In [RDR97]
an extension of the Mokum system has been described which makes it possible
to use Mokum also in a global fashion, that is in Cyberspace. In this paper we
will give a sketch of the implementation details in Sect. 3. In [GRBO97] we have
described how authorization tuples can be derived from a work flow specification
and how these can be combined with a run-time system, also using the Mokum
system. ERP systems integrate the work of employees in a company often de-
defined in work flows with their usage of databases. In [RJG98] we have studied
how security control in ERP systems is removed from the database system to
a new layer in the ERP system itself. In Sect. 4 we will briefly describe this.
In Sect. 2 we will introduce the hospital-insurance company example in more
detail. In Sect. 5 we will make the comparison between the two approaches and
give conclusions. In the area of architectures for Security & Privacy a lot of work
has been done, and it is not possible in the framework of this paper to discuss
that work here. We suffice with mentioning the Gendler & Gudes Model [GG97]
which is a model in which the epistemic principle, as we will describe in Sect.
3, can be recognized, but not the ontologic principle. Also the MOOSE system
described in [HTS97] comes close to the capability-driven approach we describe
in Sect. 4.

2 The Example

Hospital H has medical staff and administrative staff. The medical staff consists
of doctors and nurses (male and female). Patients are persons, having a medical
record which is a private object kept in a collection of which the doctor of the
patient (we assume there is only one) is the keeper. The nurse of the patient is
not allowed to access the medical record, with the exception of an emergency
and the doctor not being present. Also an employee HA in the administrative
department has access to the financial records from which he can determine
what a treatment has cost in terms of money; he sends invoices to the patients.
He is keeping the administration in patient records in collections of objects of
which he is the keeper. The Insurance company IC has several departments, one
is the claim department, with claim employee CE, which treats claims issued
by persons referring to a treatment by a doctor in H, recorded in the financial
record. We have prepared three test queries and we will see in the next sections
how they are dealt with in the two architectures.