Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science 229 (2009) 97–115

Electronic Notes in Theoretical Computer Science

www.elsevier.com/locate/entcs

Towards Secrecy for Rewriting in Weakly Adhesive Categories

Tobias Heindel

Abteilung für Informatik und angewandte Kognitionswissenschaft
Universität Duisburg-Essen
Duisburg, Germany

Abstract

Inspired by the scope extrusion phenomenon of name passing calculi that allow to reason about knowledge of (secret) names, we propose an abstract formulation of the concept of secret in any weakly adhesive category. The guiding idea is to mark part of a system state as visible or publicly accessible; further, in principle, something that has become public knowledge will stay accessible indefinitely.
The main technical contribution consists in providing a proof which shows that a recently proposed categorical construction, which produces a category having monomorphisms as objects and pullback squares as morphisms, preserves weak adhesivity. Finally we sketch how it is possible to verify certain secrecy properties using unfolding based verification approaches that lately have been generalized to rewriting systems in weakly adhesive categories.

Keywords: adhesive categories, interaction models, verification

1 Introduction

In every day communication, private information is usually exchanged only between communication partners that trust each other, as the consequences of public availability of private information tend to be numerous and subtle. In fact, more often than not, one would rather prefer that a certain piece of private information will never be become known to the public. Here we are not only talking about issues of embarrassment or reputation, but also about secret data like personal identification numbers for (on-line) banking accounts.

Nevertheless, as the example of on-line banking illustrates, there often occur situations in which secret data need to be transmitted via protected channels between trustworthy communication partners, and moreover the critical data must not become disclosed to a third party. The running example of this paper will be concerned with access keys to a private network, e.g. the intranet of some banking institute. Obviously, in this scenario, it is important that such access keys do not become publicly available.

doi:10.1016/j.entcs.2009.06.041

One of the first approaches to formally reason about the security of key exchange protocols using cryptographic methods, is the spi-calculus [1], which extends the π-calculus [14] by cryptographic primitives. Based on this name passing calculus, there has been carried out a large amount of work concerning the verification of concrete protocols. The actual protocol verification tools however do sometimes use techniques from other fields of computer science (see e.g. [3]). Alternatively, protocols might also be specified and verified using graph transformation systems [4,12]; the latter have the advantage that they are often easier understandable by laypersons.

Now the aim of this paper is *not* another concrete proposal of a modelling technique for protocols. Instead we strive for a better understanding of the fundamental distinction between private and public knowledge, which corresponds to the open/bound names dichotomy of name passing calculi. Moreover the scope extrusion phenomenon of the latter captures the possibility to exchange secret information and, in the extreme, to make secret information publicly available.

Taking a more abstract point of view, given an arbitrary state of a system, then part of of this state is open to public access (while at the same time other parts are still secret). In the process calculus world, the open part corresponds to the free names of a process. In graph transformations systems using the borrowed context approach [5], the open part is singled out by a sub-graph of the graph which models the whole system state.

The main question is now, when the private part and the public part (in the model) of a given system state should be considered "sufficiently" distinct such that all secret information is protected from public access. Though this question usually has an intuitive answer in concrete example cases, the question seems more difficult in the abstract setting of this paper, as we consider system states as objects of an arbitrary (weakly) adhesive category.

To help answer this question, we proceed as follows. First we introduce the protected links calculus as an toy example of a simple name passing calculus, which nevertheless is sufficiently rich to illustrate the private/public dichotomy and allows to give a precise characterization of *secrecy violations*. Then we give the graphical representation of this calculus in section 3. With these concrete examples at hand, in section 4, we set out to lift the notion of *secrecy violation* to the abstract setting of adhesive categories in such a way that the results of [2] apply.

2 The protected links calculus

The running example of this paper will be the protected links calculus (PLC), which couples the ideas of (the implementation of) the explicit fusion calculus [16] with a basic access control mechanism. Recall that the explicit fusion calculus was developed with the goal of providing an implementation of Milner's π-calculus [14]. The "machine model" was the fusion machine described in [16]; a simplified version of the latter has been proposed in [8], where also a "low-level" encoding of the π-calculus was presented.

Now the main characteristic of the protected links calculus that it shares with