Available online at www.sciencedirect.com

ScienceDirect

Electronic Notes in Theoretical Computer Science

ELSEVIER

Electronic Notes in Theoretical Computer Science 168 (2007) 61–75

www.elsevier.com/locate/entcs

Algorithmic Verification of Noninterference Properties[⋆]

Ron van der Meyden Chenyi Zhang

School of Computer Science and Engineering,
University of New South Wales,
Sydney, Australia

National ICT Australia,
Locked Bag 6016, Sydney,
NSW 1466, Australia

Abstract

The paper discusses the problem of model checking a number of noninterference properties in finite state systems: Noninterference, Nondeducibility on Inputs, Generalised Noninterference, Forward Correctability and Restrictiveness. The complexity of these problems is characterized, and a number of possible heuristics for optimization of the model checking are discussed.

Keywords: noninterference, model checking, complexity, heuristics

1 Introduction

The notion of 'noninterference' is a general term applied in the security literature to a number of causality-like notions intended to capture the intuition that information does not flow from high level users to lower level users, so that confidentiality of high level information is maintained. The main approach to verification that systems satisfy these properties has been proof theoretic methods using so-called 'unwinding conditions'. In this paper, we investigate the applicability of algorithmic verification techniques when the systems in question are finite state. We develop algorithms for model checking a number of different noninterference notions, and characterize the computational complexity of the associated verification problems. In particular, we deal with Noninterference on deterministic systems [12,25], Nondeducibility on Inputs [26], Generalised Noninterference [18], Forward Correctability [15] and Restrictiveness [18].

[⋆] National ICT Australia is funded through the Australian Government's *Backing Australia's Ability* initiative, in part through the Australian Research Council

doi:10.1016/j.entcs.2006.11.002

Noninterference has been studied under several distinct semantic models, including state based models [12,25], trace-set models [20,30] and process algebras [23,8]. Only for the latter has there been a systematic study of algorithmic verification of these notions [8,9]. The process algebraic models are the most expressive, and definitions of noninterference notions on other models can be reduced to definitions of noninterference notions on a process algebraic model by means of natural mappings between the models [28]. However, state based system modelling approaches are more natural to many, are likely to be adequate for many applications, have a more extensive literature on algorithmic verification, and have a more highly developed set of verification tools. This modelling approach also remains the predominant approach in operating systems verification efforts [14], the area originally motivating the noninterference literature. It therefore makes sense to consider the algorithmic verification problem also on state based models. This is particularly so with respect to complexity bounds, where lower bounds proved for a more expressive semantic model may not apply on a more restrictive model. We therefore focus in this paper on a state based modelling of systems, and (to make the verification problem decidable) restrict attention to finite state systems.

The contributions of the paper are as follows. First, we show that noninterference in deterministic systems can be reduced to a *safety* property, so it is expressible in both branching time and linear time temporal logics and verifiable in polynomial time by existing model checkers. Also in PTIME is the notion of Restrictiveness on nondeterministic systems. We show that the remaining notions of noninterference on nondeterministic systems that we consider are PSPACE-complete. For some of these notions (Restrictiveness and Nondeducibility on Inputs), these results are closely related to results of Focardi and Gorrieri [8,9] (but on a more restricted semantic model, hence not immediate consequences for the lower bounds). The results on Generalised Noninterference and Forward Correctability are new, as far as we know. Finally, we discuss heuristics that may be applied to the verification of noninterference notions, and give complexity arguments that suggest that these heuristics may sometimes lead to optimizations.

2 State-Observed Model

The state based system models in the literature on noninterference can be roughly classified into two distinct types, depending on whether observations are associated with states [21,3,24] or actions [12,25]. The system definitions are similar to those of finite state automata, with the distinction between the two types resembling the Mealy/Moore distinction. It can be shown [28] that there exist natural mappings between these two types of models that preserve all the security notions that we consider in this paper. Consequently, we consider only the state-observed modeling. The systems are input-enabled, in the sense that any action can be taken at any time. Most of the literature restricts attention to two agents High (H) and Low (L) and the security policy $L \leq H$. This policy permits information to flow from Low to High but not from High to Low. We also make this restriction here, and take