Theoretical Computer Science 706 (2018) 54–82

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Multilevel transitive and intransitive non-interference, causally ☆

Paolo Baldan [a,*], Alessandro Beggiato [b]

[a] Dipartimento di Matematica, Università di Padova, Italy
[b] IMT School for Advanced Studies Lucca, Italy

ARTICLE INFO

Article history:
Received 26 January 2017
Accepted 2 October 2017
Communicated by V. Sassone

Keywords:
Multilevel non-interference
Intransitive policies and downgrading
Petri nets
Unfolding semantics
True concurrency
Verification

ABSTRACT

We develop a theory of non-interference for multilevel security based on causality, with Petri nets as a reference model. We first focus on transitive non-interference, where the relation representing the admitted flow is transitive. Then we extend the approach to intransitive non-interference, where the transitivity assumption is dismissed, leading to a framework which is suited to model a controlled disclosure of information. Efficient verification algorithms based on the unfolding semantics of Petri nets stem out of the theory. We also argue about the possibility of performing a compositional verification.

1. Introduction

The problem of controlling the flow of information in a computing system is a classical one, faced by many contributions in the literature. A general formalization of information flow security is provided by [1] that introduces the notion of non-interference. Intuitively a security level is said not to interfere with another if what can be observed at the latter level is not affected by what happens at the former. In the simplest scenario, entities are classified according only to two levels, a *High* level, which intuitively should be confidential, and a *Low* level, which is public, and the information is allowed to flow from *Low* to *High*, but not vice-versa.

Different notions of behavior and observation lead to different non-interference properties. Originally non-interference has been studied for deterministic sequential systems, relying on a trace semantics. Since then, several variants of non-interference have been studied, dealing with concurrent and non-deterministic systems. In concurrent formalisms which offer forms of composition and synchronization, such as process calculi and Petri nets, a popular formulation of non-interference is the so-called NDC (Non-Deducibility on Composition), which looks at the system under analysis as a component, possibly interacting with the surrounding environment. It states that a process (or net) S is free of interferences whenever S running in isolation, seen from the low level, is behaviorally equivalent to S interacting with any parallel high level process (or net) that may synchronize on high actions (or transitions) [2–9]. Intuitively, this is often described by referring to some informal notion of causality – the activity at high level should not cause any visible effects on the behavior at low level – but formalized in terms of interleaving semantics.

☆ Work supported by the MIUR PRIN 2010LHT4KM project CINA and by the University of Padova project CPDA148418 ANCORE.
* Corresponding author.
E-mail addresses: baldan@math.unipd.it (P. Baldan), alessandro.beggiato@imtlucca.it (A. Beggiato).

https://doi.org/10.1016/j.tcs.2017.10.004
0304-3975/

This informal reference to causality is made formal in [7] that, relying on some previous work on non-interference notions in contact-free elementary nets (or equivalently pure safe nets) and trace nets [5], provides a causal characterization of BNDC (Bisimulation-based NDC) for Petri nets, in terms of the unfolding semantics [10]. The interest for a causal characterization is not only of theoretical nature. On the pragmatic side the use of a true concurrent semantics, like the unfolding, which represents interleaving only implicitly, is helpful to face the state explosion problem which affects the verification of concurrent systems.

Since its infancy (see, e.g., [11]) information flow security has recognized the usefulness of dealing with multilevel security domains, where the security levels are not limited to "high" and "low". In general, a domain of security levels is considered, with a relation between levels specifying the admitted flows. The transitive nature of information flow – if information flows from level A to level B and from B to C then it necessarily flows from A to C – naturally leads to work with security domains where the admitted flow relation is a partial order and a system policy of the kind no read-up, no write-down, only allowing a flow of information from lower to higher levels. The order can be total, expressing a hierarchy of confidentiality degrees (e.g., top secret, secret, confidential and unclassified in a military setting). It can also be partial, typically when various confidentiality criteria are combined into a single domain. For instance, an administration could keep public and sensitive citizen data concerning taxes and civil status. The fact that the rights of accessing sensitive tax and civil status data are independent, naturally leads to a lattice of security levels.

As argued, e.g., in [12] it can also be natural to consider security policies where the admitted flow relation is not transitive, in a way that a direct flow between two security levels, say from A to B, is forbidden, while a flow mediated through a third level, say D, is admitted. Intransitive policies are suited, for instance, for representing declassification or downgrading of confidential information. This allows for a controlled form of leakage, making such policies more realistic than pure non-interference policies that instead impose a complete isolation of confidential levels. More generally, by exploiting intransitive policies, it is possible to prescribe the (possibly cyclic) paths on which information is allowed to flow in a given system.

In this paper, building on [7,13], we provide a causal characterization of non-interference properties for (safe) Petri nets in a multilevel setting. We first focus on multilevel transitive policies and the property BNDC. Then we consider intransitive policies and the property BINI (Bisimilarity-based Intransitive Non-Interference) the adaptation of BNDC to intransitive security domains. The characterization is used to develop corresponding verification algorithms based on the unfolding semantics, that are implemented in a tool called MultiUBIC (Multi Unfolding-Based Interference Checker).

More in detail, in the transitive case a Petri net is shown to enjoy BNDC when its unfolding reveals neither a direct causality from a higher level transition to a lower level one (witnessed by a *weak causal* place), nor a direct conflict between a lower level and a higher level transition (witnessed by a *weak conflict* place). Both situations represent a violation of the policy: in the first situation, intuitively, a token produced at a higher level flows down to a lower level, while in the second situation a transition of a higher level competes for a token with one at a lower level. In the intransitive case, the characterization becomes slightly more complex: a violation of the policy is still witnessed by an influence (causality or conflict) from some level A to a level B to which the flow is not permitted, but this must not be mediated by a level where information can legitimately flow from A. Such characterizations enable the definition of algorithms that check the non-interference property on suitably defined complete prefixes of the unfolding.

Relying on the causal characterization, we also prove some compositionality properties of transitive and intransitive non-interference, that can be of help in reducing the complexity of the verification phase. In particular we show that, when a system can be decomposed as the parallel composition of subcomponents, the absence of interferences (validity of BNDC or BINI) for the entire system can be deduced from the absence of interferences in the subcomponents.

The unfolding-based algorithms are implemented in the tool MultiUBIC [14]. Compared to tools that construct (or explore) the reachability graph of the net, like ANICA (Automated Non-Interference Check Assistant) [15] and PNSC (Petri Net Security Checker) [16], the partial order representation of concurrency in MultiUBIC – as for its predecessor UBIC – leads to a gain of efficiency for highly concurrent systems where the unfolding prefix can be exponentially smaller than the complete state space (see e.g. [17]).

In the paper we also show that the verification of multilevel policies can be reduced to a number of problems on two-level security domains (possibly enriched with a downgrading level in the intransitive case). This suggests an alternative way of dealing with multilevel systems. Indeed, MultiUBIC comes equipped with facilities for performing the reduction. The experiments suggest that, in general, a direct multilevel verification is more efficient when the number of levels increases, but situations are singled out where the reduction is instead more convenient.

This paper brings to a maturity the work initiated in [7,13]. Concerning the transitive setting, we generalize [7] by developing notions, algorithms and a tool that deal with general multilevel domains rather than with two-level domains. Once the right notions are identified some parts of the extension work relatively smoothly. Hence we tried to describe only the main aspects, still keeping the paper as much as possible self-contained. Concerning the intransitive case, the paper treats general multilevel intransitive domains that include, as a special case, the two-level domains with downgrading of the conference paper [13].

The rest of the paper is organized as follows. In § 2 we define multilevel security domains and we review some basic notions for Petri nets, and their unfolding semantics. In § 3 we focus on transitive policies and the BNDC property, providing a causal characterization and a corresponding algorithm for verifying whether a safe Petri net is BNDC. In § 4 we extend the results established for BNDC to intransitive policies. In § 5 we prove some compositionality properties for BNDC and BINI. In § 6 we present the tool MultiUBIC and discuss the results of some test runs (fully detailed in Appendix B). In § 7