



A comparison of semantic models for noninterference[☆]

Ron van der Meyden ^{a,b}, Chenyi Zhang ^{a,b,c,*}

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

^b National ICT Australia, Sydney, Australia

^c Université du Luxembourg, Luxembourg

ARTICLE INFO

Article history:

Received 9 October 2008

Received in revised form 13 May 2010

Accepted 11 August 2010

Communicated by R. Gorrieri

Keywords:

Computer security

Noninterference

Information flow

Comparison

ABSTRACT

The literature on definitions of security based on causality-like notions such as noninterference has used several distinct semantic models for systems. Early work was based on state machine and trace-set definitions; more recent work has dealt with definitions of security in two distinct process algebraic settings. Comparisons between the definitions has been carried out mainly within semantic frameworks. This paper studies the relationship between semantic frameworks, by defining mappings between a number of semantic models and studying the relationship between notions of noninterference under these mappings.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

“Noninterference” is a term loosely applied in the literature to a class of formal security properties motivated from considerations of information flow and causality. Since it was invented in [6], several distinct schools have produced a variety of generalizations of the original notion, each based on their own approach to modelling systems. Existing definitions of noninterference can be roughly classified by whether they are framed in the semantic context of state based automaton models [6,28,16,23,1,27], trace based models [12,14,29,10], or process algebraic based models (further divisible into CSP [9] and CCS [15] based variants) [3,20,24].

This large diversity of models and definitions leaves a somewhat unsatisfactory situation for the potential users of this extensive literature. Noninterference originated as a proposed formalisation of information flow security in operating systems verification, a topic that has been the subject of renewed interest in recent years [27,8,19]. However, the formal systems models and definitions of security used in this area, and others, tend to be based on state based rather than process algebraic formalisms. (While the conceptual parsimony of process algebraic models is convenient for theoretical purposes, it is a disadvantage for the purpose of modelling complex systems. Most approaches to complex systems modelling used in practice treat state variables as first class citizens, and in particular, the definitions of security used in the recent operating systems work make explicit reference to state variables.) It remains unclear just what is the significance of the process algebraic work on noninterference for the application originally motivating this area of research. There have been a number of survey works and studies of the relationships between definitions in the individual process algebraic schools [24,3] but, on the whole, comparisons have been carried out within rather than across semantic frameworks. In particular, it is not clear what the impact of recent process algebraic research is for a user who prefers to work with a state based modelling.

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

* Corresponding author at: School of Computer Science and Engineering, University of New South Wales, Australia. Tel.: +61 2 8306 0488.

E-mail address: czhang@cse.unsw.edu.au (C. Zhang).

In this paper, we attempt to bridge some of the gaps between semantic models by considering the relationships between the various classical semantic models and some of the proposed notions of noninterference. We consider three types of models: two state based automaton models (introduced in Section 2) and a process algebraic framework (discussed in Section 5). The semantic intuitions underlying these frameworks are somewhat different. The automaton models have notions of “action” and of “observation”, the latter being a function of state in one case and associated to actions in the other. The process algebraic framework is seemingly more general, but diverges from the intuitions of the automaton models in that it treats both actions and observations uniformly as “active”. It is desirable to precisely understand the relationship between these frameworks. We address this question by defining formal mappings (see Sections 4 and 5) between the semantic frameworks. We study whether a variety of definitions of noninterference (introduced for the automaton models in Section 3 and for the process algebraic framework in Section 5) in the different frameworks correspond under these mappings. In particular, we identify two *distinct* transformations from an automaton theoretic framework to a CCS-like process algebraic framework. Both seem to capture reasonable idioms for the representation of the automaton theoretic notions of action and observation in process algebra.

Our results show that for several of the definitions of noninterference in the literature (viz. “nondeducibility on inputs” and “nondeducibility on strategies”), similarly named and motivated definitions in the two automaton theoretic frameworks and the process algebraic framework do correspond under the translations between these semantic frameworks. This gives a formal justification for the common naming and gives the user of older automaton theoretic definitions confidence that the process algebraic literature has not superseded older approaches in cases where an automaton based modelling is adequate for the purposes of the application. Moreover, the fact that this correspondence holds under two different mappings from automata to process algebra shows that there is some flexibility in how we can understand automaton based modellings from a process algebraic perspective.

However, matters are significantly more subtle for several other definitions of security, viz McCullough’s *restrictiveness* [12] and Bevier and Young’s notion of *Behavioural Nondeterministic Security* [1]. Both are based on a notion of *McCullough unwinding* on systems. Behavioural Nondeterministic Security is closest to the definitions of security that have been used in the literature on information flow in operating systems. This notion has been considered neither in the literature on action-observed systems, nor in process algebra, so one of the contributions of the paper is to define versions of this notion in these semantic settings.

For both restrictiveness and Behavioural Nondeterministic Security we find that while definitions of these notions in the two automaton theoretic frameworks coincide directly, for only one of our two translations from automata to process algebra does there exist a definition of restrictiveness in the process algebraic literature that corresponds under the translation. (For restrictiveness, we also find a correspondence under this translation to “strong bisimulation based nondeducibility on compositions” [3].) However, we are able to develop a novel process algebraic notion of unwinding, which we call *weak McCullough unwinding* and show that it yields new notions of security in the process algebraic setting corresponding precisely to restrictiveness and Behavioural Nondeterministic Security on automata under the second translation.

Our results highlight some differences in the understanding of action and observation in automata and process algebra. The automaton model treats observations as obligatory, and not under the control of the agent: an agent cannot avoid making an observation. On the other hand, a common understanding of process algebra treats all events of an agent as under their control. The definition of weak unwinding is stated in a way that effectively treats observations as not under the causal control of the observing agent. In defining Behavioural Nondeterministic Security in the process algebraic setting, we also need to make sense of the notion of an agent’s “most recent observation” in ways that depend on the translation being used: in one case observations in the automaton theoretic model are mapped to *potential observations* in the process algebraic model, in the other we need a notion of “most recent observation” that includes the agents most recent action. Our results show that there are, indeed, some subtleties that need to be considered very carefully when modelling a system in process algebra for purposes of security analysis.

A final aspect of our results is that we show several cases where distinct definitions of security in the process algebraic framework prove to be equivalent with respect to the range of our mappings from the state based frameworks. There has been a proliferation of definitions in the process algebraic setting, which may lead a practitioner to question which of the many new definitions is the appropriate one for their application, and to ask whether classical definitions have been supplanted by more recent work. Our results indicate that the new definitions are inherently concerned with subtle distinctions that appear only in the richly expressive framework of the process algebraic semantics. Where a system may be modelled in the less expressive state based setting, the classical definitions suffice.

The structure of the paper is as follows. In Section 2 we define the two state based semantic models we consider: state-observed and action-observed automata. Section 3 defines the range of security properties we study with respect to each of these two semantic models. In Section 4, we define mappings between these two state based models, and establish correspondences between notions of security for these two models. Section 5 defines the process algebraic semantics we consider, and defines notions of security for this semantics (including our new definitions for weak restrictiveness and Behavioural Nondeterministic Security in this setting), and shows how these notions correspond to state based notions of security under two different mappings from automata to processes. We make some concluding remarks in Section 6. The results of the paper are summarised in Fig. 8 in the conclusion. For the sake of readability we move the proofs of some auxiliary results into the Appendix.

2. State based models

The original system models used in the literature on noninterference modelled systems as a type of deterministic or nondeterministic automaton, in which multiple agents perform actions (give inputs) and make observations (receive outputs). Similarly to the Moore–Mealy distinction for finite state automata, we find two types of models, depending on whether observations are associated to states [1] or actions [23]. The original definitions assumed deterministic systems, but the focus of subsequent work has been on how to generalize the definitions to nondeterministic systems. In general, these systems are input-total, in the sense that any action can be taken at any time. In part, the motivation for this assumption is to prevent enabledness of actions being an additional channel for information flow. An input-total modelling is also the appropriate one if one takes the stance that the way that a user discovers that an action is not enabled is by attempting the action and observing in response a signal that the attempt has failed.

A nondeterministic *action-observed* state machine is a tuple of the form $M = \langle S, s_0, next, dom, A, O \rangle$, where S is a set of states, $s_0 \in S$ is the initial state, A is a set of actions, $dom : A \rightarrow D$ associates with each action an agent¹ and write D for the set of agents, and $next : S \times A \rightarrow \mathcal{P}(O \times S) \setminus \{\emptyset\}$ is a transition function. Here O is a set of observations that can be made when performing an action. Given a state $s \in S$, and an action $a \in A$, the set $next(s, a)$ is required to be non-empty. A tuple $(o, t) \in next(s, a)$ intuitively represents that on action a it is possible to make a transition from state s to state t and produce output o . Such a machine is *deterministic* if $next(s, a)$ is a singleton for all states s and actions a . In this case, the function $next$ may be replaced by two functions $step : S \times A \rightarrow S$ and $out : S \times A \rightarrow O$ such that $next(s, a) = \{(out(s, a), step(s, a))\}$ to obtain the state machine definition one finds, e.g., in [23]. A run of an action-observed system is a sequence $r = s_0(a_1, o_1)s_1(a_2, o_2)s_2 \dots (a_n, o_n)s_n \in S((A \times O)S)^*$ such that for all $1 \leq i \leq n$, $(o_i, s_i) \in next(s_{i-1}, a_i)$. A state $s \in S$ is said to be reachable if it occurs in some run. We write \mathbb{M}_{na} for the set of all nondeterministic action-observed state machines and \mathbb{M}_d for the set of deterministic action-observed state machines, where, in both cases, all states are reachable.²

A nondeterministic *state-observed* state machine is a tuple of the form $M = \langle S, s_0, next, obs, dom, A, O \rangle$ where S is a set of states; $s_0 \in S$ is the initial state; the function $next : S \times A \rightarrow \mathcal{P}(S) \setminus \{\emptyset\}$ is a transition function, such that $next(s, a)$ defines the set of states to which it is possible to make a transition when action $a \in A$ is performed at a state $s \in S$; the function $dom : A \rightarrow D$ associates an agent with each action, and the function $obs : S \times D \rightarrow O$ describes the observation made in each state by each agent. For readability, we ‘curry’ the function obs by writing $obs_u(s)$ for $obs(s, u)$ for $u \in D$ and $s \in S$. Such a state machine is deterministic if $next(s, a)$ is a singleton for all states s and actions a . In this case we may define a function $step : S \times A \rightarrow S$ by $next(s, a) = \{step(s, a)\}$. A run of a state-observed system is a sequence $r = s_0a_1s_1a_2s_2 \dots a_ns_n \in S(AS)^*$ such that for all $1 \leq i \leq n$, $s_i \in next(s_{i-1}, a_i)$. (Here we omit the representation of the observations since these may be recovered using the function obs .) A state $s \in S$ is said to be reachable if it occurs in some run. We write \mathbb{M}_{ns} for the set of all nondeterministic state-observed machines, and \mathbb{M}_s for the set of all deterministic state-observed machines where, in both cases, all states are reachable.

The most significant apparent difference between state- and action-observed machines is that, in the former, all agents make an observation when an action is performed, whereas in the latter, only the agent performing the action does so. Since the execution model is asynchronous, this means that whereas in action-observed systems, other agents would, unless they themselves act, have no knowledge that any agent has performed an action, they may come to have this information in state-observed systems even without acting. However, such a situation would often be a reason for the system to be declared insecure. The action-observed setting somewhat resembles the process algebraic setting of [2] where agents have to perform actions to synchronise with the system to achieve the effect of ‘observation’, but differs from it in that it bundles actions together with observations whereas [2] has separate notions of ‘input’ and ‘output’ actions.

3. Security properties on state based models

We now recall from the literature a number of security properties in the two types of state based systems. We study the relationships between these properties in Section 4.

3.1. Noninterference

Historically, one of the first information flow properties was (transitive) noninterference [6,7], defined with respect to deterministic machines. We base our discussion on the presentation of Rushby [23], which has been followed in many other

¹ The nomenclature ‘*dom*’ and ‘*D*’ arises from the fact that agents are also called “domains” in the literature. A domain may represent a group of distinct individual actors (e.g., all people and systems classified to access information at a particular security level). However, we are interested in the collective capabilities of such a group to act and deduce information, so it is convenient both conceptually and grammatically to think of the group as a single entity and use agentive language.

² This restriction is of significance because the definitions and results below that concern unfolding relations are sensitive to unreachable states. A system may always be restricted to its reachable component, and this operation should, intuitively, not have an impact on its security. Thus this restriction is without loss of generality.

works. Rushby defines both state-observed [22] and action-observed [23] systems, but treats them independently and does not consider any direct relations between the two. The classical definitions were cast in terms of *security policies* describing permitted information flows between an arbitrary collection of agents. Much of the subsequent literature restricts attention to the policy $L \leq H$ with two agents High (H) and Low (L), with information permitted to flow from Low to High but not from High to Low. For uniformity, we also make this restriction here, and let $A_H = \{a \in A \mid \text{dom}(a) = H\}$ and $A_L = \{a \in A \mid \text{dom}(a) = L\}$.

As noted above, in both state-observed and action-observed deterministic systems, we have a function $\text{step} : S \times A \rightarrow S$ to represent the deterministic state evolution as a result of actions. To represent the result of executing a sequence of actions, define the operation $\circ : S \times A^* \rightarrow S$, by $s \circ \epsilon = s$ and $s \circ (\alpha \cdot a) = \text{step}(s \circ \alpha, a)$ for $s \in S, \alpha \in A^*$ and $a \in A$.

With respect to the simple policy $L \leq H$, the definition of noninterference can be described in terms of the operation $\text{purge}_L : A^* \rightarrow A^*$ on sequences of actions that restricts the sequence to the subsequence of actions of L . Intuitively, the purged High actions are not allowed to lead to any effects observable to L . This is formalised as follows in the definitions of noninterference following [23], one for each type of system.

Definition 3.1. (1) A system in \mathbb{M}_{na} satisfies noninterference if it is deterministic and for all $\alpha \in A^*$ and $a \in A_L$, we have $\text{out}(s_0 \circ \alpha, a) = \text{out}(s_0 \circ \text{purge}_L(\alpha), a)$. We write NI_a for the set of such systems.

(2) A system in \mathbb{M}_{ns} satisfies noninterference if it is deterministic and if for all $\alpha \in A^*$, we have $\text{obs}_L(s_0 \circ \alpha) = \text{obs}_L(s_0 \circ \text{purge}_L(\alpha))$. We write NI_s for the set of such systems.

The definitions of noninterference in the two types of system are very similar. We show below that they can be seen to be equivalent in a precise sense.

3.2. Nondeducibility on inputs

One way of understanding the statement that H does not interfere with L in a deterministic system is stating that every sequence of H actions is compatible with the actions and observations of L . This leads to the proposal to take a similar notion as the formulation of noninterference in nondeterministic systems: an approach known as nondeducibility [25]. Nondeducibility is defined in a quite general way, in terms of a pair of views of runs. We focus here on a commonly used special case: Low's nondeducibility of High's actions.

We take an agent u 's view $\text{view}_u(r)$ of a run r to be the maximal state of information that it can have in an asynchronous system: its sequence of actions and observations reduced modulo stuttering. We begin by extending the agent's observations to runs. In action-observed systems we define the extended observation function $\text{Obs}_u^a : S((A \times O)S)^* \rightarrow (AO)^*$ for $u \in D$ by $\text{Obs}_u^a(s) = \epsilon$ and

$$\text{Obs}_u^a(r \cdot (a, o) \cdot s') = \begin{cases} \text{Obs}_u^a(r) \cdot a \cdot o & \text{if } \text{dom}(a) = u \\ \text{Obs}_u^a(r) & \text{otherwise.} \end{cases}$$

Here, taking the stance that an agent is aware of each action that it performs (so that if it performs an action twice, obtaining the same output, it knows that it has performed the action twice) we do not need to apply a stuttering reduction, and take $\text{view}_u(r) = \text{Obs}_u^a(r)$. In state-observed systems, the agent makes an observation at each state, and we define $\text{Obs}_u^s : S(AS)^* \rightarrow O^+(AO^+)^*$ by $\text{Obs}_u^s(s) = \text{obs}_u(s)$, and

$$\text{Obs}_u^s(\delta \cdot a \cdot s) = \begin{cases} \text{Obs}_u^s(\delta) \cdot a \cdot \text{obs}_u(s) & \text{if } \text{dom}(a) = u \\ \text{Obs}_u^s(\delta) \cdot \text{obs}_u(s) & \text{otherwise.} \end{cases}$$

Here the agent might make the same observation several times in a row, without an intervening action by that agent. This indicates that another agent has acted. To eliminate this timing based reasoning, in order to make the definition compatible with the assumption of asynchrony, we may take the view to be $\text{view}_u(r) = \text{Cond}(\text{Obs}_u^s(r))$ where Cond is the function on sequences that removes consecutive repetitions.

To state the definition of nondeducibility, we also require a function to extract the sequence of actions performed by an agent. We write $\text{Act}_u(r)$ for the sequence of actions performed by agent u in run r , and $\text{Act}(r)$ the sequence of all actions in r . We say that a sequence β is a *possible view* for agent u in a system M if there exists a run r of M such that $\text{view}_u(r) = \beta$. A sequence $\alpha \in A_H^*$ and a possible L view β in M are said to be *compatible* if there exists a run r of M with $\text{Act}_H(r) = \alpha$ and $\text{view}_L(r) = \beta$.

Definition 3.2. A system M satisfies Nondeducibility on Inputs if for every $\alpha \in A_H^*$, and every possible L view β in M , α is compatible with β . Write NDI_s and NDI_a for the set of systems in \mathbb{M}_{ns} and \mathbb{M}_{na} (respectively) satisfying nondeducibility on inputs.

Intuitively, this definition says that Low never learns anything about what actions High has performed.

3.3. Nondeducibility on strategies

Wittbold and Johnson [28] argued that systems classified as secure by nondeducibility on inputs may nevertheless permit flows of information flow from High to Low. They present a system in which by selecting its actions according to a particular strategy, High may directly control Low's observations. They propose an alternate definition they call "nondeducibility on strategies" which behaves more satisfactorily on the example.

The framework in which they work is synchronous state machines with simultaneous actions. Nevertheless, it is possible to formulate a similar definition in the asynchronous models defined above. In state-observed systems, we define an asynchronous High strategy to be a function $\pi : O^+(A_H O^+)^* \rightarrow A_H \cup \{\epsilon\}$ mapping each possible high view to a choice of High action or the ‘noop’ action ϵ . We say that a run $s_0 a_1 s_1 \dots a_n s_n$ is consistent with π if $\text{dom}(a_i) = H$ implies $a_i = \pi(\text{view}_H(s_0 a_1 s_1 \dots a_{i-1} s_{i-1}))$, for each $i = 1 \dots n$. Similarly, in action-observed systems, we define an asynchronous High strategy to be a function $\pi : (A_H O)^* \rightarrow A_H \cup \{\epsilon\}$. A run $s_0 (a_1, o_1) s_1 \dots (a_n, o_n) s_n$ is consistent with π if $\text{dom}(a_i) = H$ implies $a_i = \pi(\text{view}_H(s_0 (a_1, o_1) s_1 \dots (a_{i-1}, o_{i-1}) s_{i-1}))$. Given a system $M \in \mathbb{M}_{na}$ or $M \in \mathbb{M}_{ns}$ and a strategy π of the appropriate type, define

$$\text{Aview}_L(M, \pi) = \{\text{view}_L(r) \mid r \text{ is an run of } M \text{ consistent with } \pi\}.$$

Definition 3.3. M is secure wrt Nondeducibility on Strategies (written $M \in NDS_a$ or $M \in NDS_s$, according to $M \in \mathbb{M}_{na}$ or $M \in \mathbb{M}_{ns}$) if for all High strategies π, π' , $\text{Aview}_L(M, \pi) = \text{Aview}_L(M, \pi')$.

It has been shown that in synchronous systems with simultaneous inputs, Nondeducibility on Strategies is strictly stronger than Nondeducibility on Inputs [28]. However in asynchronous systems this result does not hold, and in fact we will show that the two notions coincide. Before showing the results we claimed, we need the following lemma.

Lemma 3.4. A system $M \in \mathbb{M}_{na}(\mathbb{M}_{ns})$ is in $NDI_a(NDI_s)$ iff every possible L view is compatible with $\epsilon \in A_H^*$.

Proof. The ‘only if’ direction is trivial. For the ‘if’ direction, assume that every possible L view is compatible with ϵ and let β be a possible L view.

- (1) If $M \in \mathbb{M}_{na}$, we prove by induction that for all $\alpha \in A_H^*$, there exists a run r such that $\text{view}_L(r) = \beta$ and $\text{Act}_H(r) = \alpha$. The base case when $\alpha = \epsilon$ is trivial by assumption. Suppose for some $\alpha \in A_H^*$, there is a run r satisfying $\text{view}_L(r) = \beta$ and $\text{Act}_H(r) = \alpha$, we show the case for $\alpha \cdot a$. Let s be the last state of r , then there exists $s' \in S$ such that $(o, s') \in \text{next}(s, a)$. Then we have $\text{view}_L(r(a, o)s') = \text{view}_L(r)$ by $\text{dom}(a) \neq L$, and $\text{Act}_H(r(a, o)s') = \alpha \cdot a$.
- (2) If $M \in \mathbb{M}_{ns}$, we give a similar proof by induction. The base case when $\alpha = \epsilon$ is trivial by assumption. Suppose for some $\alpha \in A^*$, there is a run r satisfying $\text{view}_L(r) = \beta$ and $\text{Act}_H(r) = \alpha$, we show the case for $\alpha \cdot a$. Let s be the last state of r , then there exists $s' \in S$ such that $s' \in \text{next}(s, a)$. We need to show that $\text{obs}_L(s) = \text{obs}_L(s')$. Suppose it were the case that $\text{obs}_L(s) \neq \text{obs}_L(s')$, then $\text{view}_L(ras') = \text{view}_L(r)\text{obs}_L(s')$ which is a sequence ending with $\text{obs}_L(s)\text{obs}_L(s')$. Then for all runs r' with $\text{view}_L(r') = \text{view}_L(ras')$, it is always the case that $\text{Act}_H(r') \neq \epsilon$ by definition of the function view , which contradicts the assumption that every possible L observation is compatible with $\epsilon \in A_H^*$. Therefore we have $\text{obs}_L(s) = \text{obs}_L(s')$, so that $\text{view}_L(ras') = \text{view}_L(r) = \beta$ and $\text{Act}_H(ras') = \alpha \cdot a$. \square

Theorem 3.5. $NDS_a = NDI_a$ and $NDS_s = NDI_s$.

Proof. To show that $NDS \subseteq NDI$ we show that if $M \notin NDI$ then $M \notin NDS$. By Lemma 3.4, M not in NDI implies there exists some possible L view β not compatible with the sequence of H actions ϵ , so β is also not consistent with the High strategy π defined by $\pi(\gamma) = \epsilon$ for all H views γ . So M is not in NDS .

To show that $NDI \subseteq NDS$, suppose that the system is in NDI . Then every possible L view β is compatible with $\epsilon \in A_H^*$, i.e., there exists a run r with $\text{view}_L(r) = \beta$ and $\text{Act}_H(r) = \epsilon$. Let π be an H -strategy, then π is consistent with r by definition. (Because it holds vacuously that $\text{dom}(a_i) = H$ implies $a_i = \pi(\text{view}_H(s_0 a_1 s_1 \dots a_{i-1} s_{i-1}))$ for all i .) This shows that the set $\text{Aview}_L(M, \pi)$ consists of all possible views of L in M , and $M \in NDS$ follows. \square

A very similar result has previously been noted in a process algebraic setting by Focardi and Gorrieri.³ Theorem 3.5 could in fact be obtained as a consequence of their results and translation results from state- and action-observed systems that we present in Section 5. Note that, by Wittbold and Johnson’s example [28], the equivalence does not hold in synchronous systems.

3.4. Unwinding-like properties

A number of the definitions in the literature on noninterference for nondeterministic systems are closely related to the following notion, that was originally motivated as a way of facilitating proofs of noninterference for deterministic systems.

Definition 3.6. An unwinding relation for an action-observed deterministic system $M \in \mathbb{M}_a$ is an equivalence relation \sim_L on the states of M satisfying the following conditions, for all states s, t and actions a ⁴:

- *Output Consistency_a:* if $a \in A_L$ and $s \sim_L t$ then $\text{out}(s, a) = \text{out}(t, a)$;
- *Locally Respects:* if $a \in A_H$ then $s \sim_L \text{step}(s, a)$;

³ See [2], in p. 20–21: Theorem 3.27 states $ND CIT = NNIIT$, and Corollary 3.29 states $NNIIT = TNDI \cap IT$. The definition of $TNDI$ resembles that of NDI , and the definition of $ND CIT$ resembles that of NDS .

⁴ We present a slight modification of the usual definition, which would have an equivalence relation \sim_u for each agent u , satisfying a similar set of conditions for each u . For the policy $L \leq H$ we can take \sim_H to be the identity relation, which automatically satisfies the necessary conditions.

- **Step Consistency:** if $a \in A_L$ and $s \sim_L t$ then $\text{step}(s, a) \sim_L \text{step}(t, a)$.

An unwinding relation for a state-observed deterministic system $M \in \mathbb{M}_s$ is an equivalence relation satisfying Locally Respects, Step Consistency, and the following variant of Output Consistency.

- **Output Consistency_s:** if $s \sim_L t$ then $\text{obs}_L(s) = \text{obs}_L(t)$.

We note that unwinding relations are sensitive to the behaviour of systems on unreachable parts of the state space. Since it is not reasonable that security of a system should depend on unreachable states, as stated before, we recall that we assume that all systems have been restricted to their reachable states.

The relationship between unwinding conditions and noninterference is given by the following classical results. (A proof of parts not explicit in the literature is given in the [Appendix](#).)

Theorem 3.7 ([7,23]). (1) If there exists an unwinding relation for a deterministic system $M \in \mathbb{M}_{na}$ ($M \in \mathbb{M}_{ns}$), then $M \in NI_a$ ($M \in NI_s$).

(2) If $M \in NI_a$ ($M \in NI_s$) then there exists an unwinding relation for M .

The following is a natural generalization of [Definition 3.6](#) to nondeterministic systems. (Note that Output Consistency has been incorporated into SC in the unwinding relation for \mathbb{M}_{na} .)

Definition 3.8. An unwinding relation for a system $M \in \mathbb{M}_{na}$ is an equivalence relation \sim_L on the states of M such that for all states s, s', t , actions a , and outputs o ,

- LR_a : if $a \in A_H$ and $(o, t) \in \text{next}(s, a)$ then $s \sim_L t$,
- SC_a : if $a \in A_L$ and $s \sim_L s'$ and $(o, t) \in \text{next}(s, a)$, then there exists a state t' such that $(o, t') \in \text{next}(s', a)$ and $t \sim_L t'$.

An unwinding relation for a system $M \in \mathbb{M}_{ns}$ is an equivalence relation satisfying

- OC_s : if $s \sim_L t$ then $\text{obs}_L(s) = \text{obs}_L(t)$,
- LR_s : if $a \in A_H$ and $t \in \text{next}(s, a)$ then $s \sim_L t$,
- SC_s : if $a \in A_L$ and $s \sim_L s'$ and $t \in \text{next}(s, a)$, then there exists $t' \in \text{next}(s', a)$ such that $t \sim_L t'$.

Several definitions of noninterference can be expressed in terms of this generalized notion of unwinding. Given the equivalence of noninterference and the existence of an unwinding relation in deterministic systems ([Theorem 3.7](#)), the following is a natural approach to the generalization of noninterference to nondeterministic systems.

Definition 3.9. $M \in \mathbb{M}_{na}$ ($M \in \mathbb{M}_{ns}$) satisfies *restrictiveness*, written $M \in RES_a$ ($M \in RES_s$), if there exists an unwinding relation for M .

The use of McCullough's [12] term "restrictiveness" in this definition is non-obvious, since the structure of our definition differs somewhat from McCullough's. We justify it later when we discuss McCullough's work in the context of the process algebraic definitions treated in [Section 5](#).

Whereas [Definition 3.9](#) obtains a definition of noninterference by asserting that *some* relation is an unwinding, we can also obtain a definition of security by requiring that a *particular* relation is an unwinding. The following is essentially from [1], and a similar definition is given in [27]. Definitions used in the recent literature on formal verification of information flow security in operating systems (e.g. [8,19]) are closely related, although these involve other aspects such as scheduling that go beyond our present asynchronous systems model.

Definition 3.10. $M \in \mathbb{M}_{ns}$ satisfies *Behavioural Nondeterministic Security* ($M \in BNS_s$) if the relation \sim_L on the states of M defined by $s \sim_L t$ if $\text{obs}_L(s) = \text{obs}_L(t)$ is an unwinding relation.

Intuitively, this definition says that L 's future observations depend only on L 's current observation and L 's future actions. This is particularly appropriate when we interpret L 's observation as L 's complete state, and wish to express that H is unable to interfere with this state. A related intuition in action-observed systems is that L 's future observations should depend only on L 's most recent observation. The literature does not appear to contain any such definition for action-observed systems, perhaps because states do not necessarily encode the most recent observation. However, by means of a transformation of the system we may obtain a behaviourally equivalent system in which states do encode the information required.

Before describing the transformation, we note that we may use the following standard notion to make precise the notion of behavioural equivalence. Given $M_1, M_2 \in \mathbb{M}_{na}$ of the forms $M_1 = \langle S_1, s_0^1, \text{next}_1, \text{dom}, A \rangle$ and $M_2 = \langle S_2, s_0^2, \text{next}_2, \text{dom}, A \rangle$, a *bisimulation* is a relation $\approx \subseteq S_1 \times S_2$, such that if $s \approx t$ and $a \in A$, then

- for all $(o, s') \in \text{next}_1(s, a)$, there exists $(o, t') \in \text{next}_2(t, a)$ such that $s' \approx t'$,
- for all $(o, t') \in \text{next}_2(t, a)$, there exists $(o, s') \in \text{next}_1(s, a)$ such that $s' \approx t'$.

Write $M_1 \approx M_2$ if there exists a bisimulation satisfying $s_0^1 \approx s_0^2$.

Bisimulation is generally thought to preserve all behavioural properties of a system that are of interest. It seems reasonable that it should also preserve security properties, but since security properties are neither safety nor liveness properties, our intuitions on this matter are somewhat less clear.⁵ The following result shows that, at least in the case of RES_a , our intuitions are upheld. (For proof, see the [Appendix](#)).

⁵ See [26] for an example where an apparently sensible security property is *not* preserved under bisimulation.

Lemma 3.11. For $M_1, M_2 \in \mathbb{M}_{na}$, if $M_1 \approx M_2$ then $M_1 \in RES_a$ iff $M_2 \in RES_a$.

We now define a transformation of action-observed systems that ensures that states encode the most recent observation made by each agent.

Definition 3.12. Let $UF : \mathbb{M}_{na} \rightarrow \mathbb{M}_{na}$ be the unfolding function such that for each $M = \langle S, s_0, next, A, dom \rangle$ the system $UF(M)$ is the restriction of the system $\langle S', s'_0, next', A, dom \rangle$ to its set of reachable states, where

- $S' = S \times (D \rightarrow O \cup \{\varepsilon_0\})$
- $s'_0 = (s_0, f_0)$ where f_0 is the function with $f_0(u) = \varepsilon_0$ for all $u \in D$
- $next' : S' \times A \rightarrow \mathcal{P}(O \times S')$ is defined as $next'((s, f), a) = \{(o, (s', f[dom(a) \mapsto o])) \mid (o, s') \in next(s, a)\}$.

Here ε_0 is a special output denoting no ‘real’ output has been observed to this moment. We use the notation $f[u \mapsto o]$ for the function g that is identical to f except that $g(u) = o$.

The intuition of this mapping is that it introduces an extra component in the state that remembers the most recent output for each agent. (The price is to blow up the state space for all these observational possibilities.) This information is extractable by the functions $lastobs_u : S' \rightarrow O$ defined by $lastobs_u((s, f)) = f(u)$ for $(s, f) \in S'$ and $u \in D$. We may now give a definition of Behavioural Nondeterministic Security on action-observed systems that captures the intuition that L behaviour should depend only on L 's most recent observation.

Definition 3.13. $M \in \mathbb{M}_{na}$ satisfies *Behavioural Nondeterministic Security* ($M \in BNS_a$) if on $UF(M)$ the relation \sim_L defined by $s \sim_L t$ if $lastobs_L(s) = lastobs_L(t)$ is an unwinding relation.

It is not difficult to see that $UF(M)$ and M are bisimilar. As argued above, it is a reasonable intuition that definitions of security should be preserved under bisimulation, so a test for security of system M stated in terms of $UF(M)$ seems justifiable. Indeed, it also follows that if M_1 and M_2 are bisimilar then so are $UF(M_1)$ and $UF(M_2)$, which further supports this claim.

We now consider how these unwinding based definitions of security are related:

Proposition 3.14. The following inclusions are proper: $BNS_a \subset RES_a \subset NDI_a$ and $BNS_s \subset RES_s \subset NDI_s$.

Proof. (1) To see that $BNS_a \subseteq RES_a$, note that if $M \in BNS_a$ then there exists an unwinding relation on $UF(M)$, thus $UF(M) \in RES_a$. It is obvious that $M \approx UF(M)$, so $M \in RES_a$ by Lemma 3.11.

To show the difference between BNS_a and RES_a , we have in Fig. 1 the system M_1 with $S = \{s_0, s_1, s_2\}$ and the transition function $next(s_i, h) = \{(0, s_i)\}$ for $i = 0, 1, 2$, $next(s_0, l) = \{(0, s_0), (0, s_1), (0, s_2)\}$, $next(s_1, l) = \{(0, s_1)\}$ and $next(s_2, l) = \{(1, s_2)\}$. Clearly $M_1 \in RES_a$ since the identity relation on S is an unwinding relation. However $M_1 \notin BNS_a$, because after performing action l from (s_0, f_0) , the system can be in either state (s_1, f) or (s_2, g) with $f(l) = g(l) = 0$, hence $(s_1, f) \sim_L (s_2, g)$, but in one case we have only observation 0 possible on action l , whereas in the other, only observation 1 is possible on action l , so \sim_L is not an unwinding relation. Thus $RES_a \not\subseteq BNS_a$.

Next we show that $RES_a \subseteq NDI_a$. Let an action-observed system M be in RES_a , witnessed by the unwinding relation \sim . Let $\beta \in (AO)^*$ be a possible L view, then there is a run $r = s_0(a_1, o_1)s_1 \dots (a_n, o_n)s_n$ of M satisfying $view_L(r) = \beta$. We only need to show that β is compatible with $\epsilon \in A_H^*$, by Lemma 3.4. We show this by induction on the length of r , proving the stronger statement that there exists a run r' with final state t such that $t \sim s_n$ and $view_L(r') = view_L(r)$ and $Act_H(r') = \epsilon$. The base case is trivial. For the inductive case, consider an extension $r_1 = r(a_{n+1}, o_{n+1})s_{n+1}$ of r . By the inductive hypothesis we have that there exists a run r' with final state t such that $t \sim s_n$ and $view_L(r') = view_L(r)$ and $Act_H(r') = \epsilon$. We need to find a run r'_1 with final state t' such that $t' \sim s_{n+1}$ and $view_L(r'_1) = view_L(r_1)$ and $Act_H(r) = \epsilon$. We consider two cases:

- Suppose first that $a_{n+1} \in A_H$. Then by LR_a we have that $s_n \sim s_{n+1}$. Since \sim is an equivalence relation it follows that $t \sim s_{n+1}$. Thus, we may take $r'_1 = r'$ and we have satisfied the required conditions, since $view_L(r_1) = view_L(r)$ in this case.
- Suppose that $a_{n+1} \in A_L$. Note that in this case, $view_L(r_1) = view_L(r)a_{n+1}o_{n+1}$. By Step Consistency, there exists $(o_{n+1}, t') \in next(t, a_{n+1})$ such that $s_{n+1} \sim t'$. Thus, we may satisfy the required conditions by taking $r'_1 = r'(a_{n+1}, o_{n+1})t'$.

The inclusion is proper: to show this we have in Fig. 1 the system M_2 with $S = \{s_0, s_1, s_2\}$ and the transition function $next(s_0, h) = \{(0, s_1)\}$, $next(s_i, h) = \{(0, s_i)\}$ for $i = 1, 2$, $next(s_0, l) = \{(0, s_1), (1, s_2)\}$, $next(s_1, l) = \{(0, s_1)\}$ and $next(s_2, l) = \{(1, s_2)\}$. It is obvious that $M_2 \in NDI_a$. Since L 's views are in the pattern $(l, 0)^* + (l, 1)^*$, let a possible L view β be $(l, x)(l, x) \dots (l, x)$ with $x \in \{0, 1\}$, then there exists a run $r = s_0(l, x)s_{x+1}(l, x)s_{x+1} \dots (l, x)s_{x+1}$ with $view_L(r) = \beta$ and $Act_H(r) = \epsilon$. But $M_2 \notin RES_a$. Suppose that \sim were an unwinding relation on M_2 . By LR_a we must have $s_0 \sim s_1$. However, $(1, s_2) \in next(s_0, l)$ but for no state t do we have $(1, t) \in next(s_1, l)$, contradicting SC_a. Therefore $NDI_a \not\subseteq RES_a$.

- (2) For state-observed systems, the result $BNS_s \subset RES_s \subset NDI_s$ can be proved in a similar way. We remark that the proof could also be derived from part (1) using the transformations F_{sa} , F_{as} , to be introduced in Section 4, that map between state- and action-observed systems, in such a way as to preserve all the security properties we have defined in this paper. \square

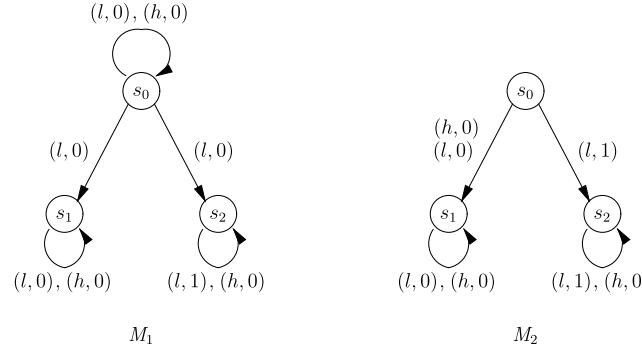


Fig. 1. Systems distinguishing BNS_a , RES_a and NDI_a .

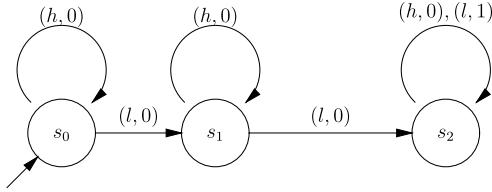


Fig. 2. A deterministic example in RES_a but not in BNS_a .

The following result shows that these notions are in fact generalizations of noninterference on deterministic systems.

Proposition 3.15. *On deterministic systems, the notions $NI_a(NI_s)$, $NDI_a(NDI_s)$ and $RES_a(RES_s)$ are equivalent.*

Proof. Since $RES_s \subseteq NDI_s$, to prove that $NI_s = NDI_s = RES_s$ on \mathbb{M}_s , we only need to show

- (1) $NDI_s \cap \mathbb{M}_s \subseteq NI_s$. Suppose $M \in NDI_s \cap \mathbb{M}_s$. Then for every possible action sequence $\alpha \in A^*$, there exists a run $r \in S(AS)^*$ with $Act(r) = \alpha$. Let its low observation $view_L(r)$ be β . Then from Lemma 3.4, β is compatible with empty H input, so there exists a run r' with $view_L(r') = \beta$ and $Act_H(r') = \epsilon$, i.e., $Act(r') = \text{purge}_L(\alpha)$. From $M \in M_s$, r and r' are the unique runs for the action sequences α and $\text{purge}_L(\alpha)$. Since they have the same L view, they agree on the last observation which is $obs_L(s_0 \circ \alpha) = obs_L(s_0 \circ \text{purge}_L(\alpha))$.
- (2) $NI_s \subseteq RES_s$. Suppose $M \in NI_s$. Then M is deterministic and from Theorem 3.7, there exists an unwinding relation \sim_L for NI_s , which can be taken to be the unwinding relation for RES_s .

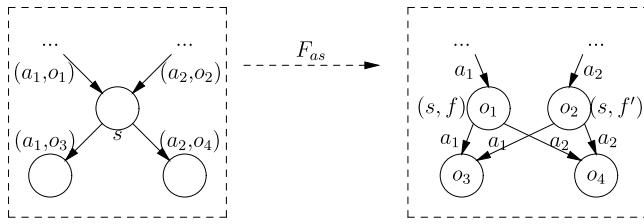
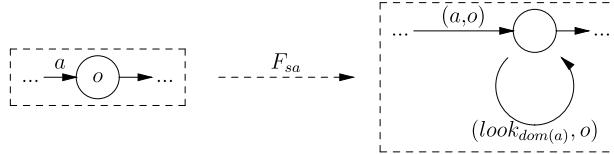
Similar results on action-observed systems can be derived from the translation results of Section 4. \square

We remark that the containment $BNS_a \subset RES_a$ is proper in deterministic systems. For an example of this, define $M = \langle S, s_0, step, out, dom, A, O \rangle$ by $S = \{s_0, s_1, s_2\}$, $A = \{l, h\}$ with $dom(h) = H$ and $dom(l) = L$, $O = \{0, 1\}$. The functions $step$ and out are defined by

- $step(s_i, h) = s_i$ and $out(s_i, h) = 0$ for $i = 0, 1$ and 2 ,
- $step(s_0, l) = s_1$ and $out(s_0, l) = 0$,
- $step(s_1, l) = s_2$ and $out(s_1, l) = 0$,
- $step(s_2, l) = s_2$ and $out(s_2, l) = 1$.

See Fig. 2. It is obvious that the identity relation on S is an unwinding relation. However, after unfolding M , on $UF(M)$ we will have $lastobs_L((s_1, f)) = lastobs_L((s_2, g)) = 0$ provided $f(L) = g(L) = 0$, but $out((s_1, f), l) = 0 \neq 1 = out((s_2, g), l)$.

In this section, we have considered four different definitions of security (in each of the two different systems models). One might be tempted to ask which of these definitions is the “right” one. We would argue that this is the wrong question. Two of the definitions (*Nondeducibility on Inputs* and *Nondeducibility on Strategies*) are both intuitive, and although they turn out to be equivalent in asynchronous systems, represent quite different assumptions about the attacker. Both deal with L 's ability to make deductions about H from its observations, but NDI assumes that L is a passive observer with no ability to control H activity, whereas NDS assumes that L may have been able to plant a Trojan horse at H , and concerns the ability of such a Trojan horse to transmit information to L . *Restrictiveness* and *Behavioural Nondeterministic Security* are arguably less intuitive, and we suggest that they are best understood as *proof techniques*. We note that when proving something about a system, it is in general preferable to prove a stronger claim than a weaker claim (subject to the degree of difficulty of the proof). From this point of view, it is entirely reasonable to prove a stronger property such as BNS , even when one is primarily interested in a property such as NDI . Although BNS has had little attention in the recent theoretical literature, it is close to the properties used in operating systems verification literature [19,8]. It is also interesting to note that RES provides a *complete* proof technique for *noninterference* on deterministic systems, by Theorem 3.7.

Fig. 3. The effect of translation F_{as} on a state.Fig. 4. The effect of translation F_{sa} on a state.

4. Transformations between state based models

We now turn to our main interest in this paper, which is to study the relationship between security properties defined over different semantic models. For this, we require translations between the two types of models. The intuition underlying the two models introduced above, that agents can both act on and observe their environment is the same, and the modelling of the dynamics of actions is very closely related. Thus, the major issue in translation is how to deal with the observations. To transform action-observed systems into state-observed systems is not too difficult: the essence has already been introduced in the unfolding construction used for BNS_u (Definition 3.12), and we need only modify this construction by erasing observations from the transitions.

Definition 4.1. Let $F_{as} : \mathbb{M}_{na} \rightarrow \mathbb{M}_{ns}$ be the translation function such that for each $M = \langle S, s_0, next, A, dom \rangle$, if $UF(M) = \langle S', s'_0, next', A, dom \rangle$ and $lastobs_u : S' \rightarrow O$ are the associated mappings to observations O , we have $F_{as}(M) = \langle S', s'_0, next'', obs, A, dom \rangle$, where

$$next''(s, a) = \{t \mid (o, t) \in next'(s, a)\}$$

and $obs(s, u) = lastobs_u(s)$.

The range of F_{as} is a proper subset of \mathbb{M}_{ns} , because in any $F_{as}(M)$, for any $u, v \in D$, u cannot modify v 's observation before v gives any input. It is plain that if M is deterministic, then so is $F_{as}(M)$, so also $F_{as} : \mathbb{M}_a \rightarrow \mathbb{M}_s$.

The effect of the translation F_{as} on a state s is illustrated in Fig. 3. Let $A_u = \{a_1, a_2\}$ for some $u \in \{H, L\}$, then for u , state s is split into two states (s, f) and (s, f') with $f(u) = o_1$ and $f'(u) = o_2$. However, (s, f) and (s, f') behave identically with respect to future observations of u .

It is also possible to translate state-observed systems to action-observed systems. An apparent obstacle, however, is that whereas in action-observed systems, an action gives a new observation only to the agent performing the action, an action in a state-observed system may also give a new observation to others. In the following definition, we handle the need to model these additional effects by mapping the state observations to *potential* observations, that would be obtained if the agent were to look at the state. Thus, we define a translation that equips each agent u with a new action $look_u$ that enables the agent to obtain its observation from the current state, without changing that state.

Definition 4.2. Let $F_{sa} : \mathbb{M}_{ns} \rightarrow \mathbb{M}_{na}$ be the function such that for each $M = \langle S, s_0, next, obs, A, dom \rangle$, we have $F_{sa}(M) = \langle S, s_0, next', A', dom' \rangle$, where:

- (1) $A' = A \cup \{look_u \mid u \in D\}$,
- (2) $next' : S \times A' \rightarrow \mathcal{P}(O \times S)$ is defined by
 - (a) $next'(s, a) = \{(o, t) \mid t \in next(s, a) \wedge o = obs_{dom(a)}(t)\}$ for $a \in A$,
 - (b) $next'(s, look_u) = \{(obs_u(s), s)\}$ for $u \in D$,
- (3) $dom' = dom \cup \{\langle look_u, u \rangle \mid u \in D\}$.

The effect of the translation F_{sa} on a state is illustrated in Fig. 4. Let $dom(a) = u$, then one additional self-transition, labelled by $(look_u, o)$ is introduced for u in the resulting action-observed system, which replaces the *obligatory* observation “ o ” by a *potential* observation.

We note that this translation produces a system with significantly more runs and views than the original state-observed system. This comes about because agents may, by failing to perform a $look$ action, omit to make an observation they would have made in the state-observed system, or may perform a $look$ action multiple times in the same state. The former, in particular, means that there exist runs in which agents have a “state of information” that would not have occurred in the state-observed system. We would not expect, therefore, that all “information theoretic” properties will be preserved by

these translations. Nevertheless, we may prove that the properties discussed above correspond under the translations. The following result can be understood as confirming a key intuition concerning security properties and observations: a system is insecure if an agent is able to obtain prohibited information. Thus, modifying the system by permitting additional runs in which agents make fewer observations and *uninformative* (e.g., repeat) observations does not change the satisfaction of the security property.

Theorem 4.3. Let \mathcal{P} be any of the properties NI, NDI, NDS, BNS, RES. Then

- (1) for all $M \in \mathbb{M}_{na}$, we have $M \in \mathcal{P}_a$ iff $F_{sa}(M) \in \mathcal{P}_s$, and
- (2) for all $M \in \mathbb{M}_{ns}$, we have $M \in \mathcal{P}_s$ iff $F_{sa}(M) \in \mathcal{P}_a$.

Proof. We show this when \mathcal{P} is one of NDI, RES or BNS. If \mathcal{P} is NI, then $NI_a(NI_s)$ coincides with $NDI_a(NDI_s)$ by Proposition 3.15, so we obtain the result from the case for NDI. Similarly, if \mathcal{P} is NDS, the result follows using the equivalence of NDI and NDS (Theorem 3.5).

If \mathcal{P} is NDI:

- (1) We first show that $M \in NDI_s$ iff $F_{sa}(M) \in NDI_a$. From Lemma 3.4, we only need to show all possible L views in M are compatible with $\epsilon \in A_H^*$ iff possible L views in $F_{sa}(M)$ are compatible with $\epsilon \in A_H^*$.

For the ‘if’ part, let $F_{sa}(M) \in NDI_a$ and let $\beta \in O^+(A_L O^+)$ be a possible L view on M . We need to show that β is compatible with $\epsilon \in A_H^*$. There exists a run r of M with $view_L(r) = \beta$. Note that in r , every transition $t \in next(s, a)$ with $a \in A_H$, has $obs_L(s) = obs_L(t)$. Otherwise if we map r to $F_{sa}(M)$ and insert $look_L$ actions at each state encountered, we get a run r' of $F_{sa}(M)$ such that $view_L(r')$ contains a subsequence $(look_L o)(look_L o')$ with $o \neq o'$. Then $view_L(r')$ is incompatible with $\epsilon \in A_H^*$, which contradicts $F_{sa}(M) \in NDI_a$.

Assume that $\beta \in O(A_L O)^*$ is a possible L view of M and let $r_0 = s_0 a_1 s_1 \dots a_n s_n$ be a run of M with $view_L(r_0) = \beta$. By Definition 4.2, $F_{sa}(M)$ has the same state space. Mapping r_0 to $F_{sa}(M)$ and adding an initial $look_L$ action, we obtain a run $r_1 = s_0 (look_L, o_0) s_0 (a_1, o_1) s_1 \dots (a_n, o_n) s_n$ of $F_{sa}(M)$, where each $o_i = obs_{dom(a_i)}(s_i)$. Taking $x_i \geq 0$ to be the index of the i th action by L in this sequence, we have $view_L(r_1) = (look_L, o_0)(a_{x_1}, o_{x_1}) \dots (a_{x_m}, o_{x_m})$. In addition, $obs_L(s_{x_j}) = obs_L(s_{x_{j+1}}) = \dots = obs_L(s_{x_{j+1}-1}) = o_{x_j}$ for all $0 \leq j \leq m$. So it is obvious that $view_L(r_1) = look_L \cdot \beta$. Since $F_{sa}(M) \in NDI_a$, $view_L(r_1)$ is incompatible with $\epsilon \in A_H^*$, so there exists a run r_2 of $F_{sa}(M)$ with $view_L(r'_2) = view_L(r_1)$ and $Act_H(r_2) = \epsilon$. We may write

$$r_2 = s_0 (look_L, o_0) s_0 (a_{x_1}, o_1) s'_1 \dots (a_{x_m}, o_m) s'_m.$$

Again by Definition 4.2, we map r_2 to M as $r_3 = s_0 a_{x_1} s'_1 \dots a_{x_m} s'_m$. It is clear that $view_L(r_3) = \beta$ and $Act_H(r_3) = \epsilon$.

For the ‘only if’ part, suppose $M \in NDI_s$ and let $\beta \in ((A_L \cup \{look_L\})O)^*$ be a possible L view on $F_{sa}(M)$. We need to show that β is compatible with $\epsilon \in A_H^*$. Let r be a run of $F_{sa}(M)$ such that $view_L(r) = \beta$. Note that every observation on β returned after a $look_L$ must be the same as the observation returned by the nearest preceding L action, otherwise this indicates that H has done something, and mapping r back to M this will contradict $M \in NDI_s$.

Define $\beta' \in ((A_L \cup \{look_L\})O)^*$ by deleting all $look_L$ pairs in β but adding the pair $(look_L, obs_L(s_0))$ at the beginning. It is clear that β' is a possible view of $F_{sa}(M)$ and if β' is compatible with ϵ then so is β . Dropping the initial $look_L$ and mapping r to M we get a run r' with $look_L \cdot view_L(r') = \beta'$. From $M \in NDI_s$ there exists a run r'' with $view_L(r'') = view_L(r')$ and $Act_H(r'') = \epsilon$. Mapping r'' back to $F_{sa}(M)$, we obtain that β' is compatible with $\epsilon \in A_H^*$. That β is compatible with ϵ immediately follows.

- (2) The proof that $M \in NDI_a$ iff $F_{as}(M) \in NDI_s$ is similar to that above, but more straightforward. For the ‘if’ part, let $\beta \in (A_L O)^*$ be a possible L view on M . Then there exists a run r_0 on M with $view_L(r_0) = \beta$. Mapping r_0 to $F_{as}(M)$, we get a run r_1 with $view_L(r_1) = \epsilon_0 \cdot \beta$, because from Definition 4.1, no agent can change the other agent’s observation on states directly. From $F_{as}(M) \in NDI_s$, there exists a run r_2 with $view_L(r_2) = \epsilon_0 \cdot \beta$ and $Act_L(r_2) = \epsilon$. Using Definition 4.1, we map r_2 back to M , obtaining a run r_3 such that $Act_L(r_3) = \epsilon$ and $view_L(r_3) = \beta$. The ‘only if’ part can be proved similarly.

If \mathcal{P} is RES:

We show that if $M \in RES_s$ iff $F_{sa}(M) \in RES_a$. We write $next$ for the transition function in M and $next'$ for the transition function in $F_{sa}(M)$.

- (1) For the ‘only if’ part. Suppose $M \in \mathbb{M}_{ns}$ is in RES_s , then there exists an equivalence relation \sim_L on M satisfying OC_s , LR_s and SC_s . Note that M and $F_{sa}(M)$ have the same set of states. We show that the same relation \sim_L satisfies the conditions LR_a and SC_a in $F_{sa}(M)$.

LR_a : Suppose $a \in A_H$ and $(o, t) \in next'(s, a)$. We need to show that $s \sim_L t$. There are two cases: $a = look_H$ and $a \in A_H$ in M . If $a = look_H$, then $t = s$ and $s \sim_L t$ follows from the fact that \sim_L is reflexive. If $a \in A_H$, then by construction of $F_{sa}(M)$ we have $t \in next(s, a)$, hence $s \sim_L t$ by LR_s .

SC_a : Suppose $a \in A_L$, $s \sim_L s'$ and $(o, t) \in next'(s, a)$ in $F_{sa}(M)$. We need to show that there exists a state t' such that $(o, t') \in next'(s', a)$ and $t \sim_L t'$. There are two cases: $a = look_L$ and $a \in A_L$ in M . If $a = look_L$ then $t = s$ and $o = obs_L(s)$. By OC_s , we have $obs_L(s) = obs_L(s')$. Thus, taking $t' = s'$, we have $(o, t') \in next'(s', a)$ and $t \sim_L t'$ as required. In the case $a \in A_L$ in M , we have $t \in next(s, a)$ and $o = obs_L(t)$. Since M satisfies SC_s , there exists $t' \in next(s', a)$ such that $t \sim_L t'$. By OC_s , this implies that $obs_L(t') = obs_L(t) = o$. Thus $(o, t') \in next(s', a)$ as required.

- (2) For the ‘if’ part, suppose $F_{sa}(M)$ is in RES_a . Then there exists an equivalence relation \sim_L on $F_{sa}(M)$ satisfying LR_a and SC_a . We show that the same relation \sim_L satisfies OC_s , LR_s and SC_s on M .

OC_s : If $s \sim_L t$, then by SC_a , s and t will have the same observation on the (unique) transition of $look_L$, so $obs_L(s) = obs_L(t)$.

LR_s : For $a \in A_H$, if $t \in next(s, a)$, then by the definition of F_{sa} there exists $(o, t) \in next'(s, a)$, and $s \sim_L t$ follows by LR_a .

SC_s : For $a \in A_L$, suppose $s \sim_s t$ and $s' \in next(s, a)$. Then from the definition of F_{sa} , $(o, s') \in next'(s, a)$ (where $o = obs_L(s')$). By SC_a , there exists a state t' such that $(o, t') \in next'(t, a)$ and $s' \sim_L t'$. By construction, $t' \in next(t, a)$, so this provides the required state.

On F_{as} , this is similar to the proof for F_{al}^1 in Theorem 5.24.

If \mathcal{P} is BNS :

- (1) We show that $M \in BNS_a$ iff $F_{as}(M) \in BNS_s$. Now $M \in BNS_a$ if $UF(M)$ with the relation $(s, f) \sim_L (t, g)$ iff $f(L) = g(L)$ satisfies the conditions LR_a and SC_a . The system $F_{as}(M)$ has the same set of states, initial states and actions as $UF(M)$, and is in BNS_s if it satisfies the conditions OC_s , LR_s and SC_s with respect to the same relation \sim_L . The transition relations $next$ on $UF(M)$ and $next'$ on $F_{as}(M)$ are related by $(o, (t, g)) \in next((s, f), a)$ iff $(t, g) \in next'((s, f), a)$ and $o = g(dom(a))$. The equivalence reduces to a straightforward comparison of the required conditions. We show that if SC_s holds in $F_{as}(M)$ then SC_a holds in $UF(M)$. Let $a \in A_L$ and $(o, (t, g)) \in next((s, f), a)$ and $(s, f) \sim_L (s', f')$. Then $(t, g) \in next'((s, f), a)$ and $o = g(dom(a))$. By SC_s , there exists $(t', g') \in next'((s', f'), a)$ such that $(t, g) \sim_L (t', g')$, i.e., $g(L) = g'(L)$. Thus, $g'(L) = o$, and we have $(o, (t', g')) \in next'((s', f'), a)$ and $(t, g) \sim_L (t', g')$, as required for SC_a . The converse and the remaining conditions are similarly straightforward and are left to the reader.

- (2) For the proof that $M \in BNS_s$ iff $F_{sa}(M) \in BNS_a$, let $M = \langle S, s_0, next, obs, A, dom \rangle$, $F_{sa}(M) = \langle S, s_0, next', A \cup \{look_H, look_L\}, dom \rangle$, and $UF(F_{sa}(M)) = \langle S', s'_0, next'', A \cup \{look_H, look_L\}, dom \rangle$. Note that $F_{sa}(M)$ has the same state space as M . We have the following properties of the constructions:

P1. for all $s, t_1, t_2 \in S$ and $a_1, a_2 \in A$ with $dom(a_1) = dom(a_2)$, if $(o_1, s) \in next'(t_1, a_1)$ and $(o_2, s) \in next'(t_2, a_2)$ then $o_1 = o_2$.

P2. For all $s \in S$, if $f_s \in O^D$ is the function with $f_s(L) = obs_L(s)$ and $f_s(H) = obs_H(s)$, then (s, f_s) is reachable in $UF(F_{sa}(M))$. The first is direct from Definition 4.2. For (P2), a straightforward induction shows that if s is reachable, then (s, g) is reachable for some g , and a further $look_L$ and $look_H$ step from this state reach (s, f_s) .

Suppose $M \in BNS_s$. Then we have the additional properties:

P3. For all $(s, f) \in S'$, if $f(L) \neq \varepsilon_0$ then $obs_L(s) = f(L)$.

P4. For all $(s, f) \in S'$, if $f(L) = \varepsilon_0$ then $obs_L(s) = obs_L(s_0)$.

For (P4), note that if (s, f) reachable from (s_0, f_0) , there exists a run in $UF(F_{sa}(M))$ of the form $(s_0, f_0)a_1(s_1, f_1)a_2(s_1, f_2) \dots a_n(s, f)$ with $a_i \in A_H$ for each $1 \leq i \leq n$. By the definition of UF and F_{sa} , $s_0a_1 \dots a_n s$ is a run of M , and it follows by LR_s that $obs_L(s) = obs_L(s_0)$. The argument for (P3) is similar, starting from the state reached by the last action of L in the run leading to (s, f) .

Since $M \in BNS_s$, the relation \sim on S defined by $s \sim t$ if $obs_L(s) = obs_L(t)$ satisfies LR_s and SC_s . We need to show the relation \sim' on S' defined by $(s, f) \sim' (t, g)$ if $f(L) = g(L)$ satisfies LR_a and SC_a in $UF(F_{sa}(M))$. Observe that if $(s, f) \sim' (t, g)$ then $s \sim t$, because if $f(L)$ and $g(L)$ are both equal ε_0 , then $obs_L(s) = obs_L(t) = obs_L(s_0)$, by (P4); else if neither equals ε_0 , then $obs_L(s) = f(L) = g(L) = obs_L(t)$, by (P3).

(a) For LR_a , if $a \in A_H \cup \{look_H\}$ it follows from the definition of UF that for all $(o, (t, g)) \in next''((s, f), a)$ we have $f(L) = g(L)$, hence $(s, f) \sim' (t, g)$.

(b) For SC_a , suppose $a \in A_L \cup \{look_L\}$ and $(s, f) \sim' (t, g)$ and $(o, (s', f')) \in next''((s, f), a)$. By the above observation, we have $obs_L(s) = obs_L(t)$, i.e., $s \sim t$. In the case $a \in A_L$, by Definitions 4.2 and 3.12, there exists $s' \in next(s, a)$ with $obs_L(s') = o$ and $f' = f[L \mapsto o]$. By BNS_s there exists $t' \in next(t, a)$ with $obs_L(t') = o$. Then we have $(o, (t', g[L \mapsto o])) \in next(t, a)$, and $(s', f') \sim' (t', g[L \mapsto o])$, as required for SC_a . In the case $a = look_L$, we have $(s', f') = (s, f[L \mapsto obs_L(s)]) \sim' (t, f[L \mapsto obs_L(t)]) \in next''((t, g), look_L)$, as required for SC_a .

If $UF(F_{sa}(M)) \in BNS_a$, then \sim' satisfies LR_a and SC_a , and we need to show that \sim satisfies LR_s and SC_s (OC_s is immediate from the definition).

(a) For LR_s , let $t \in next(s, a)$, where $a \in A_H$. By Definitions 4.2 and 3.12, and by (P2), (s, f_s) is reachable and $(o, (t, g)) \in next''((s, f_s), a)$ where $o = obs_H(t)$ and $g = f_s[H \mapsto o]$. Now, $(s, f_s) \sim' (t, g)$ and $(obs_L(s), (s, f_s)) \in next''((s, f_s), look_L)$. Thus, there exists, by SC_a , a state (t', g') such that $(obs_L(s), (t', g')) \in next''((t, g), look_L)$ and $(s, f_s) \sim' (t', g')$. By the definition of F_{sa} and UF , $next''((t, g), look_L) = \{(obs_L(t), (t, g[L \mapsto obs_L(t)]))\}$. It follows that $obs_L(t) = obs_L(s)$.

(b) For SC_s , suppose $s \sim t$. By (P2), (s, f_s) and (t, f_t) are reachable, and obviously, $(s, f_s) \sim' (t, f_t)$. If $s' \in next(s, a)$ with $a \in A_L$, by definition, $(o, (s', f_s[L \mapsto o])) \in next''((s, f_s), a)$, where $o = obs_L(s')$. Since \sim' satisfies SC_a , there exists (t', g) such that $(o, (t', g)) \in next''((t, f_t), a)$, and $(s', f_s[L \mapsto o]) \sim' (t', g)$. But, by the definition of UF and F_{sa} , the only such transition has $g = f_t[L \mapsto obs_L(t')]$, so this implies $obs_L(s') = o = obs_L(t')$ (i.e., $s' \sim t'$), and $t' \in next(t, a)$, as required for SC_s . \square

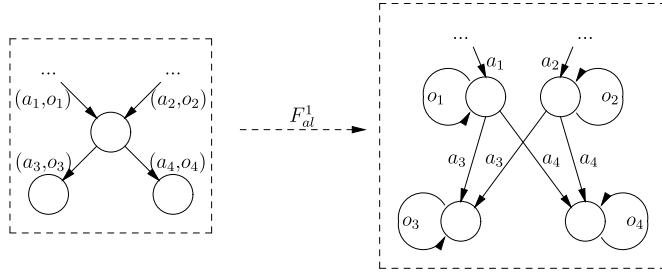


Fig. 5. The effect of translation F_{al}^1 on a state.

5. Transformations to a process algebraic model

Since the development of the original noninterference definitions, research has moved to how these definitions may be generalized to systems defined in process algebra. In this section, we study the relationships between definitions of security in the state machine models with definitions in a process algebraic setting.

5.1. Process algebraic definitions

Work on security based in process algebra has been conducted within the framework of the process algebra CSP [9], surveyed in [24], as well as the framework of a variant called SPA of the process algebra CCS [15], surveyed in [3]. We focus here on the latter, which is closer to the models considered above in that it distinguishes inputs and outputs (corresponding loosely to actions and observations). It is also cast in terms of a common semantics for both the CSP and CCS approaches, viz., labelled transition systems.

Definition 5.1. A labelled transition system (LTS) is a quadruple $M = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$ where \mathcal{L} is the set of event labels, P is the set of processes (or states), p_0 is the initial process (or state), and $\rightarrow \subseteq P \times (\mathcal{L} \cup \{\tau\}) \times P$ is the transition relation.

A run of M is a sequence $p_0 \xrightarrow{l_1} p_1 \xrightarrow{l_2} p_2 \dots p_{n-1} \xrightarrow{l_n} p_n$, and the states that occur in a run are said to be reachable. The corresponding trace of L is the sequence of labels $l_1 \dots l_n$ with any occurrences of τ deleted. We write $T(M)$ for the set of traces of M . We write \mathbb{L} for the set of all LTSs in which all states are reachable.

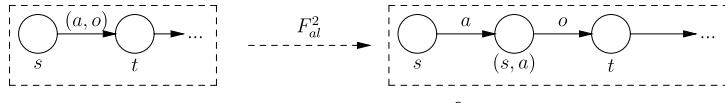
In CCS, there is also a self-inverse bijection $\bar{\cdot} : \mathcal{L} \rightarrow \mathcal{L}$ and the set of events \mathcal{L} is partitioned into a set I of input events and the set $O = \{\bar{a} | a \in I\}$ of output events. Intuitively, the input event a may synchronise with the output event \bar{a} when composing processes. We write $\mathbb{L}^{IO}(I)$ for the set of all LTS's with inputs I and corresponding set of outputs $O = \{\bar{a} | a \in I\}$, or simply \mathbb{L}^{IO} when I is clear.

In order to study security definitions, Focardi and Gorrieri [2] enhance CCS by an orthogonal partitioning of the space of events into High and Low events. Combining the two distinctions, the set \mathcal{L} of all events is thereby partitioned into High inputs (denoted HI), High outputs (HO), Low inputs (LI) and Low outputs (LO). They call the resulting process calculus SPA.

Apparently, labelled transition systems are more general than the state machine models discussed above, in that inputs are not always enabled. Superficially, SPA's labelled transition systems seem closest to action-observed state machines, inasmuch as both inputs (actions) and outputs (observations) are associated to transitions. Given the equivalences discussed above, we therefore focus on translating action-observed machines into SPA. However, whereas action-observed machines combine an action and an observation into a single state transition, SPA separates the two notions. This leaves open several plausible translations from \mathbb{M}_{na} to \mathbb{L}^{IO} . One follows an approach like that used above for the translation from \mathbb{M}_{na} to \mathbb{M}_{ns} , and treats the observations as optional events which do not change the state. We assume in the following that the sets of possible H and L observations in an action-observed system are disjoint. This is without loss of generality, since we may always rename the H observations, which does not affect any of the notions of security, since these do not refer to H observations. Similarly, we assume that the sets of actions and observations are disjoint. (Note the H and L actions are already separated by the function dom .)

Definition 5.2. Let $F_{al}^1 : \mathbb{M}_{na} \rightarrow \mathbb{L}^{IO}$ be the mapping such that if $M = \langle S, s_0, next, dom, A \rangle$, we have $F_{al}^1(M)$ is the restriction to its reachable states of $\langle P, p_0, \rightarrow, \mathcal{L} \rangle$ where

- (1) $P = S \times (O \cup \{\varepsilon_H, \varepsilon_L\})^D$,
- (2) $p_0 = (s_0, f_0)$ where f_0 is the function with $f_0(L) = \varepsilon_L$ and $f_0(H) = \varepsilon_H$,
- (3) $\mathcal{L} = I \cup O$ with $I = A$,
- (4) $(s, f) \xrightarrow{l} (t, g)$ iff either $l = a \in A$ and for some $o \in O$ we have $(o, t) \in next(s, a)$ and $g = f[dom(a) \mapsto o]$, or $(t, g) = (s, f)$ and $l = f(u)$ for some $u \in D$ and $f(u) \in O$.

Fig. 6. The effect of translation F_{al}^2 on a state.

The effect of translation F_{al}^1 on a single state is illustrated in Fig. 5, where the state in the middle of the left-hand side is split into two states with different self-transitions for the observations o_1 and o_2 .

Another approach to the translation, which keeps observations obligatory, is to introduce for each state s and action a a new state (s, a) to represent that the action a has been taken from state s , but the corresponding observation has not yet been made. This translation is depicted in Fig. 6.

Definition 5.3. Let $F_{al}^2 : \mathbb{M}_{na} \rightarrow \mathbb{L}^{lo}$ such that for $M = \langle S, s_0, \text{next}, \text{dom}, A \rangle$, we have $F_{al}(M) = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$ where

- (1) $P = S \cup (S \times A)$,
- (2) $p_0 = s_0$,
- (3) $\mathcal{L} = I \cup O$ with $I = A$,
- (4) $\rightarrow = \{(s, a, (s, a)) \mid s \in S, a \in A\} \cup \{((s, a), o, t) \mid (o, t) \in \text{next}(s, a)\}$.

Focardi and Gorrieri discuss the condition of input-totality in the context of relating their definitions of security on SPA processes to classical definitions. An LTS $M \in \mathbb{L}^{lo}(I)$ is *input-total* if for all $s \in P$ and for all $a \in I$, there exists $t \in P$ such that $s \xrightarrow{a} t$. It is apparent that for all $M \in \mathbb{M}_{na}$, the LTS $F_{al}^1(M)$ is input-total, but the LTS $F_{al}^2(M)$ is *not* input-total, since inputs are not accepted in the intermediate states (s, a) . We will discuss below the impact this difference has on the relationship between definitions of security in \mathbb{M}_{na} and \mathbb{L}^{lo} .

We now state a number of the definitions of security discussed by Focardi and Gorrieri. Given a trace t of an LTS in \mathbb{L}^{lo} , we write $\text{low}(t)$ for the subsequence of labels in $LI \cup LO$, $\text{high}(t)$ for the subsequence of labels in $HI \cup HO$, and $\text{highinput}(t)$ for the subsequence of labels in HI . We extend these functions to apply pointwise to sets of traces. We call a sequence in $\text{low}(T(M))$ a *possible low view* of M .

Definition 5.4. $M \in \mathbb{L}^{lo}$ is secure wrt Nondeterministic Noninterference ($M \in \text{NNI}_l$) if for every possible low view $\alpha \in \text{low}(T(M))$, there exists a trace $t \in T(M)$ such that $\text{low}(t) = \alpha$ and $\text{highinput}(t) = \epsilon$ is the null sequence.

This definition permits the trace t to contain high outputs. The following stronger definition prohibits this.

Definition 5.5. $M \in \mathbb{L}^{lo}$ is secure wrt Strong Nondeterministic Noninterference ($M \in \text{SNNI}_l$) if for every possible low observation $\alpha \in \text{low}(T(M))$, there exists a trace $t \in T(M)$ such that $\text{low}(t) = \alpha$ and $\text{high}(t) = \epsilon$ is the null sequence.

The following is a formulation of nondeducibility on inputs in \mathbb{L}^{lo} .

Definition 5.6. $M \in \mathbb{L}^{lo}$ is secure wrt Nondeducibility on Inputs ($M \in \text{NDI}_l$) if for every $\alpha \in HI^*$, for every possible low view $\beta \in \text{low}(T(M))$, there exists a trace $t \in T(M)$ such that $\text{low}(t) = \beta$ and $\text{highinput}(t) = \alpha$.

Finally, we have a definition that is motivated as a generalization of nondeducibility on strategies. This can be phrased⁶ in terms of a process composition with synchronisation on High events, which we formulate as follows. Given LTSs $M_1 = \langle P_1, p_1, \rightarrow_1, \mathcal{L}_1 \rangle$ and $M_2 = \langle P_2, p_2, \rightarrow_2, \mathcal{L}_2 \rangle$, define the composition $M_1 \parallel_H M_2 = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$ with states $P = P_1 \times P_2$, initial state $p_0 = (p_1, p_2)$, labels $\mathcal{L} = \mathcal{L}_1 \cup \mathcal{L}_2$, and transitions defined by $(s, t) \xrightarrow{l} (s', t')$ if either $l \in LI \cup LO$ and one of $s \xrightarrow{l} s'$ and $t = t'$ or $s = s'$ and $t \xrightarrow{l} t'$, or else $l = \tau$ and there exists events l_1, l_2 in $HI \cup HO$ such that $l_1 = \overline{l_2}$ and $s \xrightarrow{l_1} s'$ and $t \xrightarrow{l_2} t'$.

Definition 5.7. $M \in \mathbb{L}^{lo}$ is secure wrt Nondeducibility on Compositions ($M \in \text{NDC}_l$) if for every $M' \in \mathbb{L}^{lo}$ that has labels in $HI \cup HO$ only, we have $\text{low}(T(M)) = \text{low}(T(M \parallel_H M'))$.

Intuitively, process composition is used here to capture the effect of High executing a strategy in the system M . In effect, the definition compares two different behaviours of High, since the term M represents the effect of High not constraining its behaviour in any way, whereas $M \parallel_H M'$ represents the behaviours resulting when High restricts its behaviour to one that may synchronise with M' .

The range of quantification for M' in this definition is arguably too large, since it encompasses processes that may refuse to synchronise with High output events in M , by not having the corresponding input event enabled. Prima facie, it would seem that this is an issue for comparisons with nondeducibility on strategies in the system models discussed above, where there is no way for an agent to refuse an observation. Focardi and Gorrieri also consider the following variant NDCIT , which constrains the LTSs in question to be input-total. We define this in terms of a looser notion $\text{NDC}(IT)_l$, to separate input-totality of the system itself from input-totality of the composed systems.

⁶ We simplify the presentation of Focardi and Gorrieri to minimize the amount of process algebraic notation that we need to introduce.

Definition 5.8. $M \in \mathbb{L}^{10}(HI \cup LI)$ is secure wrt Nondeducibility on Compositions with Input-Total systems ($M \in NDC(IT)_I$) if for every input-total $M' \in \mathbb{L}^{10}(HI)$, we have $low(T(M)) = low(T(M \parallel_H M'))$. Define $M \in NDCIT_I$ if M is itself input-total and $M \in NDC(IT)_I$.

Intuitively, restricting M' to be input-total ensures that M' cannot block any H output events from M in the composed system $M \parallel_H M'$.

5.2. Nondeducibility based definitions

We are now ready to begin investigating the relationship between the definitions of security in action-observed systems and \mathbb{L}^{10} , under the transformations defined above. In this subsection we deal with nondeducibility based definitions. Later subsections treat restrictiveness and BNS.

Concerning nondeducibility on inputs, we obtain the following.

Theorem 5.9. For all systems $M \in \mathbb{M}_{na}$ we have $M \in NDI_a$ iff $F_{al}^1(M) \in NDI_l$ iff $F_{al}^2(M) \in NDI_l$.

Proof. (1) We show that $M \in NDI_a$ iff $F_{al}^1(M) \in NDI_l$. Suppose that $M \in NDI_a$. Let $\beta_0 \in low(T(F_{al}^1(M)))$ be a possible L view of $F_{al}^1(M)$ and let α be any sequence of H inputs, i.e., $\alpha \in HI^*$. To show $F_{al}^1(M) \in NDI_l$ we need to show that there exists a trace t with $low(t) = \beta_0$ and $highinput(t) = \alpha$. Since $\beta_0 \in low(T(F_{al}^1(M)))$ there exists a run of $F_{al}^1(M)$ with trace t_0 and $low(t_0) = \beta_0$. Note first that we still have a trace if we delete any HO events, since, by construction of $F_{al}^1(M)$, these do not change the state.

Note the following property of $F_{al}^1(M)$: if $a \in LI$, $o \in LO$ and $\gamma_2 \in (HI \cup HO \cup LO)^*$ and γ_1, γ_3 are any sequences of labels, then $\gamma_1 a \gamma_2 o \gamma_3$ is a trace iff $\gamma_1 a o \gamma_2 \gamma_3$ is a trace. This follows from the fact that transitions with labels in $HO \cup LO$ do not change the state and for transitions $(s, f) \xrightarrow{a} (s', f')$ with $a \in HI$ we have $f'(L) = f(L)$.

Thus, we may ensure that there is a LO event immediately after each $LI = A_L$ event, and delete any other LO events (including ε_L events). Let t_1 be the resulting trace and $\beta_1 = low(t_1)$. Then $\beta_1 \in (A_L O)^*$, and any consecutive pair $ao \in A_L O$ in this sequence corresponds in the witnessing run to a sequence of transitions $(s, f) \xrightarrow{a} (t, g) \xrightarrow{o} (t, g)$. This means that $(o, t) \in next(s, a)$ in M , and it follows that β_1 is a possible low view in M . Thus, by the assumption that $M \in NDI_a$, there exists a run r of M with $view_L(r) = \beta_1$ and $Act_H(r) = \alpha$. Mapping r to $F_{al}^1(M)$ by including a self-transition for each observation, we obtain a run of $F_{al}^1(M)$ with trace t_2 such that $low(t_2) = \beta_1$ and $highinput(t_2) = \alpha$. We now note that this trace can be modified into a trace t_3 with $low(t_3) = \beta_0$ and $highinput(t_3) = \alpha$ by application of the property of $F_{al}^1(M)$ noted above.

Conversely, suppose $F_{al}^1(M) \in NDI_l$ and let β be a possible L view of M and $\alpha \in A_H^*$. The run of M witnessing β maps directly over to a run of $F_{al}^1(M)$ with trace t such that $low(t) = \beta$. Thus, there exists a run of $F_{al}^1(M)$ with trace t_2 with $low(t_2) = \beta$ and $highinput(t_2) = \beta$. Since output events do not change the state in $F_{al}^1(M)$, we may assume that there are no HO events. Similarly, using the property of $F_{al}^1(M)$ noted above, we may assume that each LI event is followed immediately by an LO event, and these are the only LO events in t_2 . The run now immediately translates back to a run r' of M with $view_L(r') = \beta$ and $Act_H(r') = \alpha$.

(2) The proof that $M \in NDI_a$ iff $F_{al}^2(M) \in NDI_l$ is similar, but more straightforward, since each run on M can be directly translated into a trace on $F_{al}^2(M)$ and vice versa. \square

Thus, both transformations produce LTS representations of the system that are equivalent with respect to the property of nondeducibility on input. Since nondeducibility on strategies is equivalent to nondeducibility on input on \mathbb{M}_{na} , this result gives us a way of checking the former property through a mapping to \mathbb{L}^{10} . However, it remains of interest to check whether the notion of nondeducibility defined on \mathbb{L}^{10} corresponds to that on \mathbb{M}_{na} . This is particularly so as Focardi and Gorrieri show that the placement of nondeducibility on composition with respect to the other properties is somewhat sensitive to the class of systems to which it is applied, and the class of systems used in the compositions. Focardi and Gorrieri prove the following relationships:

Proposition 5.10 ([2]). (1) $NDC_l = SNNI_l \subset NNI_l$, and

(2) $NDI_l \subset NNI_l$

(3) $NDI_l \not\subseteq NDC_l$ and $NDC_l \not\subseteq NDI_l$

(4) $NDC_l \cap IT = NNI_l \cap IT = NDI_l \cap IT$.

We add to this the following result, which clarifies the relationship between these notions and $NDCIT = NDC(IT)_l \cap IT$.

Proposition 5.11. $NDC(IT)_l = NNI_l$ and $NDC_l \cap IT = NDC(IT)_l \cap IT$.

Proof. To see that $NDC(IT)_l \subseteq NNI_l$, suppose that $M \in NDC(IT)_l$. Let $M' = \sum_{a \in HI} a.M'$ be the input-total process that accepts all H outputs from M but itself generates no H outputs, (i.e., inputs to M). Since $M \in NDC(IT)_l$ we have $low(T(M)) = low(T(M \parallel_H M'))$. Thus, for all low views $\beta \in low(T(M))$, there exists a run r of $M \parallel_H M'$ with $low(r) = \beta$. Since M' contains no HO events, any τ events of r must arise as the combination of a HO event from M and a HI event

from M' ; no HO events from M can have been used in r . Hence, r arises from a run r' of M such that $low(r') = \beta$ and $highinput(r') = \epsilon$, as required for $M \in NNI_l$.

Conversely, for $NNI_l \subseteq NDC(IT)_l$, suppose that $M \in NNI_l$. Let M' be any input-total High process. To show that $M \in NDC(IT)_l$, we prove that $low(T(M)) \subseteq low(T(M\|_H M'))$; the converse is obvious. Let $\beta \in low(T(M))$. Since $M \in NNI_l$, there exists a run r of M with $low(r) = \beta$ and $highinput(r) = \epsilon$. This means that the only H events in r are HO events, which synchronise with HI events in M' . Since M' is input-total, we can construct from r a run r' of $M\|_H M'$, in which the HO events are replaced by τ , and which satisfies $low(r') = \beta$.

We now obtain that $NDC_l \cap IT = NDC(IT)_l \cap IT$ from the fact that $NDC(IT)_l = NNI_l$ and Proposition 5.10(4). \square

That is, on input-total systems, input-total High processes have the same discriminative powers as all processes. Using the fact that F_{al}^1 produces input-total LTSs, the equivalence of NDS_a and NDI_a and the facts from the previous two propositions, we obtain a direct correspondence between nondeducibility on strategies and several notions of nondeducibility on composition.

Corollary 5.12. *For $M \in \mathbb{M}_{na}$, we have $M \in NDS_a$ iff $F_{al}^1(M) \in NDCIT_l$ iff $F_{al}^1(M) \in NDC(IT)_l$ iff $F_{al}^1(M) \in NDC_l$.*

This means that on input-total systems, and hence on the range of F_{al}^1 , the notions NDC_l , $NDC(IT)_l$, $NDCIT_l$, NDI_l and NNI_l collapse. Although the processes produced by the translation F_{al}^2 are not input-total, there turns out to be similar correspondence for F_{al}^2 . A number of technical reasons are responsible for this. One contributing factor is the following intuitive notion.

Say that a process is *High-reactive* if for all traces t , if $highinput(t) = \epsilon$ then $high(t) = \epsilon$. Intuitively, this says that no High output is produced before any High input has been received. Proposition 5.10(1) states that $SNNI_l$ is strictly stronger than NNI_l . On High-reactive processes, the distinct notions NNI_l and $SNNI_l = NDC_l$ are identical. This follows from the following fact.

Proposition 5.13. *If M is High-reactive then $M \in NNI_l$ implies $M \in SNNI_l$.*

Proof. Suppose $M \in NNI_l$. Let β be any low view of M . Then by $M \in NNI_l$ there exists a trace t of M with $highinput(t) = \epsilon$. Since M is High-reactive, we in fact have $highinput(t) = \epsilon$, as required for $M \in SNNI_l$. \square

It is evident that processes of the form $F_{al}^2(M)$ for $M \in \mathbb{M}_{na}$ are High-reactive, so it follows that $F_{al}^2(M) \in NNI_l = NDC(IT)_l$ iff $F_{al}^2(M) \in SNNI_l = NDC_l$. Furthermore, these processes have a somewhat more technical property that also implies that $F_{al}^2(M) \in NDl_l$ iff $F_{al}^2(M) \in NNI_l$, viz., that they allow insertion of an arbitrary sequence of high inputs near the end of any trace, without perturbing the low view or preventing the occurrence of a final low input. This is made more precise in the proof of the following result.

Proposition 5.14. *For $M \in \mathbb{M}_{na}$, if $F_{al}^2(M) \in NNI_l$ then $F_{al}^2(M) \in NDl_l$.*

Proof. Suppose $F_{al}^2(M) \in NNI_l$. As just noted, this also implies that $F_{al}^2(M) \in SNNI_l$. Let β be any low view of M and let α be any sequence of High inputs. Since $F_{al}^2(M) \in SNNI_l$ there exists a run r of $F_{al}^2(M)$ with $low(r) = \beta$ and $high(r) = \epsilon$. We consider two cases. If the final state of r is a state of M , then since M is input-total, we may extend r by a sequence of High input and High output transitions to produce a run r' with the property that $low(r') = \beta$ and $highinput(r') = \alpha$, as required for $F_{al}^2(M) \in NDl_l$. Otherwise, since $high(r) = \epsilon$, we may write $r = r_1at$, where $a \in LI$ and r_1 ends in a state of M . In this case, we first extend r_1 by a sequence of High input and High output transitions based on the inputs α , and ending at a state in M after the final High output, and then take one further step by input a . This again produces a run r' with $low(r') = \beta$ and $highinput(r') = \alpha$, as required. \square

Together, these results establish the following, similar to Corollary 5.12 (except that $NDCIT_l$ is excluded since $F_{al}^2(M)$ is not input-total).

Corollary 5.15. *For $M \in \mathbb{M}_{na}$, we have $F_{al}^2(M) \in NDl_l$ iff $F_{al}^2(M) \in NDC_l$ iff $F_{al}^2(M) \in NDC(IT)_l$.*

These results show that under either representation of action-observed systems, there is significant flexibility in the range of quantification of the composed processes in the definition of nondeducibility on composition. In the action-observed representation, the notion NDS_a quantifies over deterministic strategies, i.e. strategies in which the H action is a function of H 's view of the system. In the two LTS representations, the quantification over strategies corresponds to a quantification over H processes, but there is no such determinism requirement. Still, the definitions correspond, and we may moreover choose to quantify over input-total or arbitrary H processes, without changing the satisfaction of the security property in this class of systems.⁷

⁷ Note that it is not hard to show that replacing *deterministic* strategies by *nondeterministic* strategies does not increase H 's power to restrict L 's possible views. For every nondeterministic H strategy, there always exists a deterministic H -strategy that is consistent with fewer L views. Therefore if an L view is consistent with all deterministic H strategies it will be consistent with all nondeterministic H strategies as well.

5.3. Restrictiveness

We now turn to McCullough's notion of 'restrictiveness', already mentioned above. There are two versions of 'restrictiveness' introduced in McCullough's early works. The former [11] is a trace based definition, while the latter is defined on labelled transition systems [12,13]. In [13] McCullough mentions both definitions and concludes that the one on labelled transition systems is a stronger notion. The cleanest presentation of the LTS version occurs in [13]. Here we present this definition in the pattern used for unwinding properties for the automaton models above.

Definition 5.16. Define a *McCullough unwinding relation* for an LTS M without τ transitions to be an equivalence relation \sim on the states of M such that

- M1: for all states s, s', t and input sequences α and α' such that $\alpha|LI = \alpha'|LI$, $s \xrightarrow{\alpha} s'$ and $s \sim t$, there exists a state t' such that $s' \sim t'$ and $t \xrightarrow{\alpha'} t'$;
- M2: for all states s, s', t and output sequences α such that $s \xrightarrow{\alpha} s'$ and $s \sim t$, there exists a state t' and an output sequence α' such that $\alpha|LO = \alpha'|LO$, $t \xrightarrow{\alpha'} t'$, and $s' \sim t'$.

Using this notion, we may state McCullough's definition of restrictiveness in [13] as follows.

Definition 5.17. An LTS M is *restrictive* ($M \in RES_l$) if it is input-total, it has no τ transitions, and there exists a McCullough unwinding relation for M .

We may note that in fact part of the assumption of input-totality follows from the rest of this definition, since the existence of a McCullough unwinding implies input-totality with respect to High inputs. (To see this at state s take $\alpha = \epsilon$ and $\alpha' = h$ for a High action h , and apply M1 with $s' = t = s$.)

The assumption of input-totality is often made in the literature, on the intuitive grounds that it ensures that enabledness of inputs cannot be a cause of information flow. On the other hand, input-totality might be argued to be too strong a condition. In particular, note that our translation F_{al}^2 produces systems that are *necessarily not* input-total, since inputs are not enabled at states of the form (s, a) . This means that no system $F_{al}^2(M)$ will be classified as secure according to the definition RES_l , which is undesirable.

In fact, there is a second reason why no system in the range of F_{al}^2 can satisfy RES_l . Let s be a state in $F_{al}^2(M)$ for some action-observed system M with action $a \in A_H$ enabled. Then, by the translation, any action $b \in A_L$ must be enabled on s as well. If $F_{al}^2(M)$ is in RES_l , then there is a McCullough unwinding relation \sim on $F_{al}^2(M)$, which must satisfy $s \sim (s, a)$ (to see this, take $\alpha = a$ and $\alpha' = \epsilon$ in M1). However, while b is enabled on s , it is not enabled on (s, a) , so we cannot satisfy condition M1.

The most reasonable response to this observation depends on one's intuitions concerning outputs. On the one hand, in the process algebraic literature, a common understanding is that the agent observing an output plays an active (e.g., handshake) role in its occurrence. From a security perspective, this means that a receiver can transmit information to a sender, simply by refusing to participate in the handshake. On this view, the above definition of restrictiveness may be reasonable.

On the other hand, it is also sensible to understand outputs/observations as events that "happen to", or "are available to" agents, but which they are powerless to prevent. This is implicitly the view taken in our automaton based models, and it has also been taken in the process algebraic literature: e.g., the *signal events* of [20] are intended to capture this intuition. On this view, it is too strong a condition to ask that the Low input b be enabled both at s and (s, a) in $F_{al}^2(M)$ (for a a High input), since High cannot block the reception of its output from the state (s, a) , after which the system reaches a state where b is in fact enabled. We are therefore motivated to formulate a novel revised version of unwinding and restrictiveness that is compatible with this latter perspective.

Definition 5.18. A *weak McCullough unwinding relation* is an equivalence relation \sim , such that

- W1: for all $a \in HI$, $s \xrightarrow{a} t$ implies $s \sim t$,
- W2: for all $a \in HO$, $s \sim t$ and $s \xrightarrow{a} s'$, there exists $\alpha \in HO^*$ and $t' \in S$ such that $t \xrightarrow{\alpha} t'$ and $s' \sim t'$,
- W3: for all $a \in L$, $s \sim t$ and $s \xrightarrow{a} s'$, then there exists $\alpha, \beta \in HO^*$ and $t' \in S$, such that $s' \sim t'$, and $t \xrightarrow{\alpha \cdot a \cdot \beta} t'$.

Intuitively, W1 says that High inputs do not affect Low, W2 allows that Low may be aware that High is receiving some outputs (it could even be aware of exactly what these outputs are), and W3 says that Low is aware of its own events. However, note that in W3, we do not require that Low events can be directly traced, but only modulo the occurrence of the HO events that H is powerless to block. The relationship between this definition and the previous one is expressed in the following result, whose proof is straightforward.

Lemma 5.19. A McCullough unwinding relation is also a weak McCullough unwinding relation.

Note that the converse is not true even for input-total systems. To understand this, consider the following system, depicted in Fig. 7. Let $S = \{s, t, r\}$, $LI = \{l\}$, $LO = \{o, o'\}$, $HI = \emptyset$ and $HO = \{o_H\}$. The transition relation is defined as

- $s \xrightarrow{l} s$, $s \xrightarrow{l} r$, $t \xrightarrow{l} t$ and $r \xrightarrow{l} r$
- $s \xrightarrow{o} s$, $t \xrightarrow{o} t$ and $r \xrightarrow{o'} r$,
- $s \xrightarrow{o_H} t$ and $t \xrightarrow{o_H} s$.

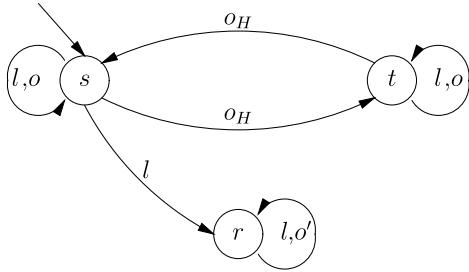


Fig. 7. An example to show the difference between McCullough and weak McCullough unwinding relations.

There exists a weak McCullough unwinding on this system, viz. the smallest equivalence relation \sim such that $s \sim t$. (This satisfies W1 trivially because $HI = \emptyset$. For W2, we need only consider two cases: (1) $s \sim t$ and $s \xrightarrow{o_H} t$ and (2) $t \sim s$ and $t \xrightarrow{o_H} s$. In case (1) we take $\alpha = o_H$ and have $t \xrightarrow{o_H} s$ and $t \sim s$, as required. Case (2) is symmetric. For W3, suppose that $a \in L$ and we have states $x \sim y$ and a transition $x \xrightarrow{a} x'$. If $x' = x$ then we may take $y' = y$ and we will have that $y \xrightarrow{a} y'$ and $x' \sim y'$ for all possible values of x and y . If $x' \neq x$ then we must have $x = s$ and $x' = r$, so $y = s$ or $y = t$. If $y = s$ we take $\alpha = \beta = \epsilon$, and if $y = t$ we take $\alpha = o_H$ and $\beta = \epsilon$, and obtain in either case that $y \xrightarrow{\alpha:\beta} r$ and $x' = r \sim r$, as required for W3.)

On the other hand, the relation \sim is not a McCullough unwinding relation. If it were, taking $\alpha = \alpha' = l$ and considering $s \sim t$ and $s \xrightarrow{l} r$, by M1 we would need to have $r \sim t$, since $t \xrightarrow{\alpha'} t'$ implies $t' = t$. But $r \sim t$ does not hold.

Based on the notion of weak McCullough unwinding (and dropping the assumption of input-totality), we obtain the following notion of security.

Definition 5.20. An LTS M is *weakly restrictive* ($M \in RES_l^w$) if it has a weak McCullough unwinding relation.

This definition has an appropriate relationship to nondeducibility based definitions such as NDI_l and NDS_l , even on systems that are not input-total, in that the following holds:

Lemma 5.21. If $M \in RES_l^w$ then for all traces α of M there exists a trace β with $\text{view}_l(\alpha) = \text{view}_l(\beta)$ and $\text{highinput}(\beta) = \epsilon$.

Note also that by Lemma 5.19, we have the following:

Corollary 5.22. If $M \in RES_l$ then $M \in RES_l^w$.

We remark that Focardi and Gorrieri [2] have also proposed a definition of restrictiveness in the context of all SPA processes. Like the definition of RES_l above, they also require input-totality. In addition to dealing with τ transitions, their definition requires that a distinction be made between high and low level τ transitions, for reasons that are not made clear. Since our translations do not produce LTSs with τ transitions, we will not attempt to treat this extension here; without it, their definition amounts to RES_l as we have defined it. It is worth remarking that Focardi and Gorrieri classify their definition of restrictiveness with the other *trace based* properties they consider. We point out that a better comparison is with the separate hierarchy of *bisimulation based* definitions of security they define. The following is one of the notions in this hierarchy.

Definition 5.23. $M \in \mathbb{L}^{IO}$ satisfies *strong bisimulation nondeducibility on compositions* (SBNDC) if for every $p \in P$ reachable from p_0 , if $p \xrightarrow{h} p'$ for some $h \in H$ then $p||_H 0 \approx_B p'||_H 0$.

Here, \approx_B is the weak bisimulation, and “0” is the deadlock process, with the usual definitions in CCS [15].

We may show the following result, that establishes a correspondence between notions of restrictiveness on action-observed systems and labelled transition systems under the translation F_{al}^1 . We note that this result justifies the use of the term restrictiveness in Definition 3.9.

Theorem 5.24. (1) $M \in RES_a$ iff $F_{al}^1(M) \in RES_l$ iff $F_{al}^1(M) \in RES_l^w$ iff $F_{al}^1(M) \in SBNDC$.
(2) $M \in RES_a$ iff $F_{al}^2(M) \in RES_l^w$.

This result (together with Theorem 4.3) shows that on the state based models, the (usually quite complicated) definition of “restrictiveness” has a rather intuitive formulation with a very clear relationship to the classical unwinding theory for noninterference on deterministic state based systems. Moreover, this notion corresponds exactly with SBNDC under one of our translations.

To prove Theorem 5.24, we first establish a number of lemmas. We first note that although, in general, restrictiveness is stronger than weak restrictiveness, we can identify situations where the two notions coincide. In particular, the following result shows that this is the case for High input-total systems in which observation transitions do not change the state; note that this condition applies to the LTSs generated by our translation F_{al}^1 .

Lemma 5.25. Suppose $M \in \mathbb{L}$ satisfies (1) for all states s, t and output events o , $s \xrightarrow{o} t$ implies $s = t$, and (2) $s \xrightarrow{a} t$ for all states s and H inputs a . Then $M \in \text{RES}_l$ iff $M \in \text{RES}_l^w$.

Proof. See the Appendix. \square

Next, weak unwinding can be given a simpler characterisation on the image of the mapping F_{al}^2 .

Lemma 5.26. For every action-observed system M , $F_{al}^2(M) \in \text{RES}_l^w$ iff there exists an equivalence relation \approx on the states of $F_{al}^2(M)$ such that

- W1': for all $a \in H$, $s \xrightarrow{a} t$ implies $s \approx t$,
- W2': for all $a \in L$, if $s \approx t$ and $s \xrightarrow{a} s'$, then there exists $\alpha \in HO^*$ and a state t' such that $s' \approx t'$ and $t \xrightarrow{\alpha \cdot a} t'$.

Proof. See the Appendix. \square

We are now in a position to prove Theorem 5.24.

Proof (Theorem 5.24). For (1), $F_{al}^1(M) \in \text{RES}_l$ implies $F_{al}^1(M) \in \text{RES}_l^w$ is direct from Lemma 5.19. It therefore suffices to show that (A) $M \in \text{RES}_a$ implies $F_{al}^1(M) \in \text{RES}_l$, that (B) $F_{al}^1(M) \in \text{RES}_l^w$ implies $F_{al}^1(M) \in \text{SBNDC}$, and that (C) $F_{al}^1(M) \in \text{SBNDC}$ implies $M \in \text{RES}_a$. Let $M = \langle S, s_0, \text{next}, \text{dom}, A \rangle$ and $F_{al}^1(M) = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$.

(A) For the argument from $M \in \text{RES}_a$ to $F_{al}^1(M) \in \text{RES}_l$, suppose $M \in \text{RES}_a$. Then there exists an unwinding relation $\sim \subseteq S \times S$. First, $F_{al}^1(M)$ is input-total. Define $\approx \subseteq P \times P$ by $(s, f) \approx (s', f')$ if $s \sim t$ and $f(L) = f'(L)$. We show that \approx is a McCullough unwinding relation.

- (1) If $(s, f) \approx (s', f')$ and for any $\alpha, \alpha' \in I^*$ with $\alpha|L = \alpha'|L$, $(s, f) \xrightarrow{\alpha} (t, g)$ it can be easily shown by induction on α and α' by the properties LR_a and SC_a of the unwinding relation \sim , that there exists (t', g') such that $(s', f') \xrightarrow{\alpha'} (t', g')$ and $(t, g) \approx (t', g')$.
- (2) The output condition is trivial because all output transitions in $F_{al}^1(M)$ are self-transitions.

(B) To show that $F_{al}^1(M) \in \text{RES}_l^w$ implies $F_{al}^1(M) \in \text{SBNDC}$, suppose $F_{al}^1(M) \in \text{RES}_l^w$. Then there exists a weak McCullough unwinding relation \sim on the states of $F_{al}^1(M)$. Given a reachable state p and $p \xrightarrow{a} p'$ for $a \in A_H$, we need to show that $p||_H 0 \approx_B p'||_H 0$. If $a \in HO$ then $p = p'$, and the claim trivially holds. If $a \in HI$ then we have $p \sim p'$. We need to show the relation \approx defined by $p||_H 0 \approx p'||_H 0$ if $p \sim p'$ is a weak bisimulation. Since there are no τ transitions, we only need to check the case when $p||_H 0 \xrightarrow{b} q||_H 0$ for some $b \in A_L$. By definition of weak McCullough unwinding there exists $p' \xrightarrow{\alpha \cdot b \cdot \beta} q'$ and $q \sim q'$ for some $\alpha, \beta \in HO^*$. However in $F_{al}^1(M)$ all outputs only produce self-transitions, thus we have $p' \xrightarrow{b} q'$ and $q \sim q'$. Therefore we have shown that $q||_H 0 \approx q'||_H 0$, i.e., \approx is a weak bisimulation as required. Thus $p||_H 0 \approx_B p'||_H 0$. By definition, $F_{al}^1(M) \in \text{SBNDC}$.

(C) For the argument from $F_{al}^1(M) \in \text{SBNDC}$ to $M \in \text{RES}_a$, suppose $F_{al}^1(M) \in \text{SBNDC}$. We first define $\sim' \subseteq S \times S$ by $s \sim' t$ if there exist $f, g \in O^D$ such that $f(L) = g(L)$, both (s, f) and (t, g) are reachable, and $(s, f)||_H 0 \approx_B (t, g)||_H 0$. This relation is reflexive and symmetric, but need not be transitive. Define \sim as the transitive closure of \sim' . Then \sim is an equivalence relation. We show that \sim is an unwinding relation on M .

LR_a : Suppose $s, t \in S, a \in A_H$ and $(o, t) \in \text{step}(s, a)$. Let $f \in O^D$ be such that (s, f) is reachable in $F_{al}^1(M)$. From Definition 5.2, $(s, f) \xrightarrow{a} (t, f[H \mapsto o])$, and since $F_{al}^1(M) \in \text{SBNDC}$, we have $(s, f)||_H 0 \approx_B (t, f[H \mapsto o])||_H 0$. Moreover, $f(L) = f[H \mapsto o](L)$, so we have $s \sim' t$, hence $s \sim t$.

SC_a : Suppose $s \sim t, a \in A_L$ and $(o, s') \in \text{step}(s, a)$. We need to show that there exists a state t' such that $(o, t') \in \text{step}(t, a)$ and $s' \sim t'$. Since $s \sim t$, there exists some $n \in \mathbb{N}^+$ such that $s(\sim')^n t$. We proceed by induction on n , showing that if $s(\sim')^n t, a \in A_L$ and $(o, s') \in \text{step}(s, a)$, then there exists a state t' such that $(o, t') \in \text{step}(t, a)$ and $s'(\sim')^n t'$. The base case of $n = 0$ is trivial. Suppose that $s(\sim')^n u \sim' t, a \in A_L$ and $(o, s') \in \text{step}(s, a)$. By the induction hypothesis, there exists a state u' such that $(o, u') \in \text{step}(u, a)$ and $s'(\sim')^n u'$. Since $u \sim' t$, there exist $f, g \in O^D$ such that (u, f) and (t, g) are reachable, $f(L) = g(L)$ and $(u, f)||_H 0 \approx_B (t, g)||_H 0$. By the construction of $F_{al}^1(M)$, we have $(u, f) \xrightarrow{a} (u', f[L \mapsto o])$. Thus, there exists a transition $(t, g) \xrightarrow{a} (t', g')$ such that $(u', f[L \mapsto o])||_H 0 \approx_B (t', g')||_H 0$. But there exists a transition labelled o from $(u', f[L \mapsto o])$, so there must also exist a transition labelled o from (t', g') . The construction of $F_{al}^1(M)$ implies that $g'(L) = o = f[L \mapsto o](L)$. This shows that $u' \sim' t'$. Since, also by construction of $F_{al}^1(M)$, we have $(o, t') \in \text{next}(t, a)$, this gives the required transition and relation in M to complete the proof.

For (2), let $F_{al}^2(M) = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$ with $P = S \cup (S \times A)$, $p_0 = s_0$, $\mathcal{L} = I \cup O$ and $\rightarrow = \{(s, a, (s, a)) \mid s \in S, a \in A\} \cup \{(s, a, o, t) \mid (o, t) \in \text{next}(s, a)\}$. We show that $M \in \text{RES}_a$ implies $F_{al}^2(M) \in \text{RES}_l^w$. Let \sim be an unwinding relation on M . Define a symmetric relation $\approx_0 \subseteq P$, by the following:

- (1) For $s, t \in S$, if $s \sim t$ in M then $s \approx_0 t$.
- (2) For $s, t \in S, a \in HI$ and $o \in HO$, if $s \xrightarrow{a} (s, a) \xrightarrow{o} t$, then $s \approx_0 (s, a)$ and $(s, a) \approx_0 t$.
- (3) For $s, t \in S$ and $a \in LI$, if $s \sim t$ then $(s, a) \approx_0 (t, a)$.

Define \approx as the reflexive, transitive closure of \approx_0 . Then \approx is an equivalence relation. We prove that \approx satisfies conditions W1' and W2' in Lemma 5.26. The proof of W1' is trivial from rule (2). For W2', we first show that the relation \approx_0 satisfies the following:

(*) If $u_1 \approx_0 u_2$ and $u_1 \xrightarrow{\alpha \cdot e} u'_1$ for $\alpha \in HO^*$ and $e \in L$ then there exists $\alpha' \in HO^*$ and a state u'_2 such that $u_2 \xrightarrow{\alpha' \cdot e} u'_2$ and $u'_1 \approx_0 u'_2$.

The proof of W2' is then straightforward. Suppose $a \in L$, $u \approx v$ and $u \xrightarrow{a} u'$. Then there exist $u_0, u_1, \dots, u_n \in P$ such that $u_{i-1} \approx_0 u_i$ for all $i = 1 \dots n$, $u = u_0$ and $v = u_n$. By induction using (*), we obtain a sequence of states $u' = u'_0, \dots, u'_n$ and sequences $\alpha_1, \dots, \alpha_n \in HO^*$ such that $u_i \xrightarrow{\alpha_i \cdot a} u'_i$ and $u'_{i-1} \approx_0 u'_i$. It follows by transitivity that $u' \approx u'_n$ and $v \xrightarrow{\alpha_n \cdot a} u'_n$, as required for W2'.

For the proof of (*), suppose that $u_1 \approx_0 u_2$ and $u_1 \xrightarrow{\alpha \cdot e} u'_1$ for $\alpha \in HO^*$ and $e \in L$. We have the following cases:

- If $u_1 \approx_0 u_2$ by rule 1, then $u_1, u_2 \in S$ and $u_1 \sim u_2$. By construction of $F_{al}^2(M)$, the only possibilities for the transition $u_1 \xrightarrow{\alpha \cdot e} u'_1$ are $e \in LI$, $\alpha = \epsilon$ and $u'_1 = (u_1, e)$. Since then $u_2 \xrightarrow{\epsilon \cdot e} (u_2, e)$, and $(u_1, e) \approx_0 (u_2, e)$ by rule 3, we may take $\alpha' = \epsilon$ and $u'_2 = (u_2, e)$.
- If $u_1 \approx_0 u_2$ by rule 2, then we have the following cases.
 - Suppose $u_1 = s$ and $u_2 = (s, b)$ for some $s \in S$ and $b \in HI$, then the only possibility for $u_1 \xrightarrow{\alpha \cdot e} u'_1$ is $s \xrightarrow{\epsilon \cdot a} (s, a)$ with $e = a \in LI$. Let $(o, t) \in next(s, b)$ for some $o \in HO$, then $s \sim t$ in M by LR_a . Therefore $t \xrightarrow{a} (t, a)$ and $(s, a) \approx_0 (t, a)$ by rule 3. Combining the previous H output we have $u_2 = (s, b) \xrightarrow{o \cdot a} (t, a)$ and $(s, a) \approx_0 (t, a)$, so we may take $\alpha' = o$ and $u'_2 = (t, a)$.
 - The reverse of the previous case: $u_1 = (s, b)$ and $u_2 = s$ for some $b \in HI$. Here the only possibility for $u_1 \xrightarrow{\alpha \cdot e} u'_1$ is $(s, b) \xrightarrow{o} t \xrightarrow{a} (t, a)$ for some $t \in S$, $\alpha = o \in HO$ and $e = a \in LI$. Therefore in M we have $(o, t) \in next(s, b)$, and $s \sim t$ by LR_a . So we have $s \xrightarrow{\epsilon \cdot a} (s, a)$ and $(t, a) \approx_0 (s, a)$ by rule 3. Here we may take $\alpha' = \epsilon$ and $u'_2 = (s, a)$.
 - Suppose $u_1 = (s, b)$ and $u_2 = t$ with $(s, b) \xrightarrow{o} t$ for $b \in HI$ and $o \in HO$. Then the only possibility for $u_1 \xrightarrow{\alpha \cdot e} u'_1$ is $(s, b) \xrightarrow{o} t \xrightarrow{a} (t, a)$ with $\alpha = o$ and $e = a \in LI$. Since $t \sim t$ in M , we have $t \xrightarrow{\epsilon \cdot a} (t, a)$ and $(t, a) \approx_0 (t, a)$ by rule 3, so we may take $\alpha' = \epsilon$ and $u'_2 = (t, a)$.
 - The reverse of the previous case: $u_1 = t$, $u_2 = (s, b)$ and $(s, b) \xrightarrow{o} t$ for $b \in HI$ and $o \in HO$. Now the possibility for $u_1 \xrightarrow{\alpha \cdot e} u'_1$ is $t \xrightarrow{\epsilon \cdot a} (t, a)$ with $\alpha = \epsilon$ and $e = a \in LI$. Then $(s, b) \xrightarrow{o \cdot a} (t, a)$ and $(t, a) \approx_0 (t, a)$ by rule 3, so we may take $\alpha' = o$ and $u'_2 = (t, a)$.
- If $u_1 \approx_0 u_2$ by rule 3, then u_1 and u_2 are in the form of (s, a) and (t, a) , respectively, with $s \sim t$ and $a \in LI$. Then the only possibility for $u_1 \xrightarrow{\alpha \cdot e} u'_1$ is that $u_1 = (s, a) \xrightarrow{\epsilon \cdot o} s' = u'_1$ with $e = o \in LO$, so $(o, s') \in next(s, a)$. By $s \sim t$ and SC_a , there exists $(o, t') \in next(t, a)$ such that $s' \sim t'$. Therefore $s' \approx_0 t'$ by rule 1 and $u_2 = (t, a) \xrightarrow{\epsilon \cdot o} t'$. Thus, we may take $\alpha' = \epsilon$ and $u'_2 = t'$.

This completes the proof of (*). \square

Next we show that $F_{al}^2(M) \in RES_l^w$ implies $M \in RES_a$. Suppose that there is a relation \approx on $F_{al}^2(M)$ as defined in Lemma 5.26. We define $s \sim t$ in M if $s \approx t$ in $F_{al}^2(M)$. Then obviously \sim is an equivalence relation since \approx is an equivalence relation. To show that \sim is an unwinding relation, we argue as follows:

- LR_a : for all $a \in A_H$ and $(o, t) \in next(s, a)$, we have $s \xrightarrow{a} (s, a) \xrightarrow{o} t$ in $F_{al}^2(M)$, so $s \approx t$ by W1' and transitivity, which implies $s \sim t$.
- SC_a : if $s \sim t$, $a \in A_L$ and $(o, s') \in next(s, a)$ then $s \approx t$ and we have $s \xrightarrow{a} (s, a) \xrightarrow{o} s'$ in $F_{al}^2(M)$. By W2', there exists $\alpha' \in HO^*$ and a state u such that $t \xrightarrow{\alpha' \cdot a} u$ and $(s, a) \approx u$. Since no actions in HO are enabled on t the only possibility for $t \xrightarrow{\alpha' \cdot a} u$ is $\alpha' = \epsilon$ and $t \xrightarrow{\epsilon \cdot a} (t, a)$, so we have $(s, a) \approx (t, a)$. By a similar argument using W2' from $(s, a) \approx (t, a)$ and $(s, a) \xrightarrow{o} s'$, we conclude that there exists a state $t' \in S$ such that $(t, a) \xrightarrow{o} t'$ and $s' \approx t'$, hence $s' \approx t'$. By the definition of F_{al}^2 , we have $(o, t') \in next(t, a)$ and $s' \sim t'$. \square

We note that the function F_{al}^2 does not make $F_{al}^2(M) \in RES_l^w$ coincide $F_{al}^2(M) \in SBND$ in that every H input must be followed by an H output in the translated system, while $SBND$ requires that $s \xrightarrow{a} t$ implies $s \approx_B t$ for all reachable s and $a \in H$, thus it does not distinguish inputs and outputs from H .

It is also worth noting that we relate the RES properties to $SBND$ but not $BNDC$. This is because in some cases $BNDC$ does not guarantee deducibility based security. The following process Q ,

$$Q = \tau.l_1.Q + l_2.l_2.Q + h_1.l_1.Q$$

a variant of one discussed in Forster's thesis [4], can be verified to satisfy SBSSI and BNDC, but L's observation of (a single) l_2 is incompatible with H's action h_1 . Therefore, in general, BNDC is incomparable with deducibility based security properties such as NDI_L .

5.4. BNS

For completeness, we also characterise the notion BNS, [1] discussed above, within LTS. The intuition for BNS is that Low's future pattern of observations depends only on the current Low state, which, in the context of action-observed system, we took to be Low's most recent observation.

We found in the previous section that restrictiveness on action-observed systems corresponds to two different notions of security on labelled transition systems, depending on whether we translate from action-observed systems using F_{al}^1 or F_{al}^2 , since these translations construct labelled transition systems with somewhat different intuitive interpretations. A similar point applies to the notion BNS. In order to formulate BNS on labelled transition systems, we need to make sense of the notion of "most recent observation" of an agent, so that we may define BNS by stating (using a notion of unwinding) that Low's new observation on performing an action depends only on its most recent observation and the action being performed (the dependency on the later is implicit in the definitions above).

In the case of F_{al}^1 , we have the difficulty that the translation constructs LTSs that generate some runs in which an agent performs a sequence of actions but never makes an observation. However, the missing observations in such runs were enabled as self-loops from the states generated during the execution. The appropriate intuitive viewpoint to take to this would seem to be that an agent is able to observe the set of outputs enabled at a state. (This makes the most intuitive sense when output transitions are self-transitions. It is also quite reasonable if different observations represent, e.g., the values of variables that an agent may read.)

For a state p of an LTS $\langle P, p_0, \rightarrow, \mathcal{L} \rangle$, define $obs_L(p)$ to be the set of $o \in LO$ such that there exists $p' \in P$ with $p \xrightarrow{o} p'$. Using this definition we obtain the following definition of BNS in labelled transition systems.

Definition 5.27. An LTS M is in BNS_L if the relation \sim_L , defined on M by $p \sim_L q$ if $obs_L(p) = obs_L(q)$, is a McCullough unwinding.

The intuition for the relation \sim_L on LTSs (equivalence of the set of possible observations) is somewhat different from that used in the definition of BNS_a (equivalence of the most recent L observation). However, in $F_{al}^1(M)$, the (unique) next possible observation is in fact that which would have been obtained from the most recent L action. Thus, it is not surprising to find the following equivalence.

Theorem 5.28. If $M \in \mathbb{M}_{na}$ then $M \in BNS_a$ iff $F_{al}^1(M) \in BNS_L$.

Proof. Let $M = \langle S, s_0, next, dom, A \rangle$, $F_{al}^1(M) = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$, and $UF(M) = \langle S', (s_0, f_0), next', dom, A \rangle$. First, note that $UF(M)$ and $F_{al}^1(M)$ have the same set of states. Moreover, we have $(s, f) \sim_L (t, g)$ (in $UF(M)$), iff $f(L) = g(L)$ iff $obs_L((s, f)) = \{f(L)\} = \{g(L)\} = obs_L((t, g))$ iff $(s, f) \sim_L (t, g)$ (in $F_{al}^1(M)$). Thus also the equivalence relations in question are identical and we need to show that \sim_L is an unwinding relation on $UF(M)$ iff \sim_L is a McCullough unwinding on $F_{al}^1(M)$.

We prove that \sim_L is an unwinding relation on $UF(M)$ if \sim_L is a McCullough unwinding on $F_{al}^1(M)$.

LR_a For all $(o, (t, g)) \in next'((s, f), a)$ with $a \in A_H$, $g = f[H \mapsto o]$, so $g(L) = f(L)$ which implies $(s, f) \sim_L (t, g)$.

SC_a For all $(s, f), (t, g) \in S'$ with $(s, f) \sim_L (t, g)$ and $(o, (s', f')) \in next'((s, f), a)$ with $a \in A_L$, by definition, $f'(L) = o$, and

on M , $(o, s') \in next(s, a)$. Thus, $(s, f) \xrightarrow{a} (s', f')$ in $F_{al}^1(M)$. Since \sim_L is a McCullough unwinding relation, and $a \in LI$, there exists a transition $(t, g) \xrightarrow{a} (t', g')$ with $(s', f') \sim_L (t', g')$. Thus $g'(L) = f'(L) = o$. This means that there exists a transition $(o, t') \in next(t, a)$ in M , hence $(o, (t', g')) \in next((t, g), a)$ in $UF(M)$.

From \sim_L being an unwinding relation to \sim_L being a McCullough unwinding can be proved by first doing an induction on the length on any input sequence $\alpha, \alpha' \in (LI \cup HI)^*$ with $\alpha|LI = \alpha'|LI$. The output case is trivial and similar to what was shown in the proof of Theorem 5.24. \square

In case of the systems produced by F_{al}^2 , we do not have the problem that outputs are optional, so we can make sense of the notion of "most recent observation" straightforwardly as "the label of the output transition most recently taken". However, this translation produces two different types of states: those of the form s of the system being translated (where no outputs are enabled) and those of the form (s, a) (where only a single output is enabled). Since their behaviour with respect to Low outputs differs, we cannot treat these two types of states as equivalent under an unwinding. In order to define a reasonable notion of BNS on such systems, we therefore take the view that an agent is aware of its most recent observation, as well as any actions it has taken since that observation (allowing multiple such actions makes the definition applicable to a more general set of LTSs than those produced by F_{al}^2).

To formalise these ideas, we use the following notion of unfolding, which produces a version of an LTS in which states record the most recent observation and any subsequent actions. For $M = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$ an LTS with inputs I and outputs O , let the unfolding of M be

$$UF_I(M) = \langle P \times (OI^* \cup I^*)^D, (p_0, f_0), \rightarrow, \mathcal{L} \rangle$$

restricted to the set of reachable states, where f_0 is the function satisfying $f_0(u) = \epsilon$ for all $u \in D$. The transition relation is defined as $(s, f) \xrightarrow{a} (t, g)$ if $s \xrightarrow{a} t$ in M , and

- if $a \in I$, then $g = f[\text{dom}(a) \mapsto f(\text{dom}(a)) \cdot a]$,
- if $a \in O$, then $g = f[\text{dom}(a) \mapsto (a)]$.

Intuitively, the function f records each agent's information about the most recent observation and any subsequent actions. On taking an action we append this action to the agent's record; on an observation we update the record to consist of just that observation.

Using this notion of unfolding, we may now state a definition of BNS on LTSs that is appropriate to the LTSs produced by the transformation F_{al}^2 . As discussed above in the context of restrictiveness, the notion of unwinding that is most appropriate to such systems is weak McCullough unwinding. This leads to the following definition.

Definition 5.29. $M \in \mathbb{L}$ is in BNS_l^w if the relation \sim on $UF_l(M)$, defined by $(u, f) \sim (v, g)$ iff $f(L) = g(L)$, is a weak McCullough unwinding relation.

This notion corresponds to BNS_a in the desired way:

Theorem 5.30. $M \in BNS_a$ iff $F_{al}^2(M) \in BNS_l^w$.

In the proof of this result, we need to establish the relationship between two systems connected by F_{al}^2 when they are both unfolded (though in two different ways). Given $M = \langle S, s_0, \text{next}, A, \text{dom} \rangle \in \mathbb{M}_{na}$ and $F_{al}^2(M) = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$, define the following equivalence relations

- \sim on the states $S \times (O \cup \{\epsilon_0\})^D$ of $UF(M)$ by $(s, f) \sim (t, g)$ iff $f(L) = g(L)$, and
- \sim' on the states $P \times (OA^* \cup A^*)^D$ of $UF_l(F_{al}^2(M))$ by $(s, f') \sim' (t, g')$ iff $f'(L) = g'(L)$.

We have the following observation.

Lemma 5.31. For all $s, t \in S$, there exist reachable states (s, f) and (t, g) in $UF(M)$ such that $(s, f) \sim (t, g)$ iff there exists reachable states (s, f') and (t, g') in $UF_l(F_{al}^2(M))$ such that $(s, f') \sim' (t, g')$.

Proof. For the ‘only if’, if (s, f) is reachable in $UF(M)$ then there is a run $(s_0, f_0)(a_1, o_1)(s_1, f_1) \dots (a_n, o_n)(s_n, f_n)$ with $(s, f) = (s_n, f_n)$. Then by the definition of UF^L and F_{al}^2 , there is a run

$$(s_0, f'_0) a_1 ((s_0, a_1), f'_1) o_1 (s_1, f'_1) \dots ((s_{n-1}, a_n), f'_n) o_n (s_n, f'_n)$$

of $UF^L(F_{al}^2(M))$ with $s = s_n$. If there exists a rightmost L action a_i in this run, then $f'_n(L) = o_i = f_n(L)$. Otherwise $f'_n(L) = \epsilon$ and $f_n(L) = \epsilon_0$. We let f' be f'_n . Similarly by tracing a run reaching (t, g) in $UF(M)$, we construct another run in $UF^L(F_{al}^2(M))$ reaching (t, g') with either $g'(L) = o_i = g(L) = f(L)$ or $g(L) = \epsilon_0 = f(L)$ and $g'(L) = \epsilon$. Therefore we have the existence of f' and g' with $f'(L) = g'(L)$, so $(s, f') \sim' (t, g')$. The proof for the ‘if’ part is similar. \square

We can now give the proof of Theorem 5.30:

Proof. Let $M = \langle S, s_0, \text{next}, A, \text{dom} \rangle$, and $F_{al}^2(M) = \langle P, p_0, \rightarrow, \mathcal{L} \rangle$ with $P = S \cup (S \times A)$. Note that in the LTSs $F_{al}^2(M)$ and $UF_l(F_{al}^2(M))$ we consider, we have $LI = A_L$ and $HI = A_H$.

For the ‘only if’ part, suppose $M \in BNS_a$. We show that on $UF_l(F_{al}^2(M))$ the relation \sim' , defined by $(u, f) \sim' (v, g)$ if $f(L) = g(L)$, is a weak McCullough unwinding relation.

- W1. If $(u, f) \xrightarrow{a} (u', f')$ with $a \in HI$, then $f' = f[H \mapsto f(H) \cdot a]$, and $f'(L) = f(L)$, therefore $(u, f) \sim' (u', f')$.
- W2. Suppose $(u, f) \xrightarrow{a} (u', f')$ with $a \in HO$, and $(u, f) \sim' (v, g)$. Then $f' = f[H \mapsto a]$, and therefore $f'(L) = f(L) = g(L)$. We satisfy the requirements of W2 using $(v, g) \xrightarrow{\epsilon} (v, g)$ and $(u', f') \sim' (v, g)$.
- W3. Suppose $(u, f) \xrightarrow{a} (u', f')$ with $a \in L$, and $(u, f) \sim' (v, g)$. We need to show that there exists $(v, g) \xrightarrow{\alpha \cdot a \cdot \alpha'} (v', g')$ with $\alpha, \alpha' \in HO^*$ and $(u', f') \sim' (v', g')$. We consider first the case where $a \in LI$. Then $u \in S$ by definition of the function F_{al}^2 . There are two cases as follows.

- If $v \in S$, then by $(u, f) \sim' (v, g)$ we have $f(L) = g(L)$. Since a is enabled on v we have $(v, g) \xrightarrow{a} (v', g')$ and $g' = g[L \mapsto g(L) \cdot a]$. It is obvious that $f'(L) = f(L) \cdot a = g(L) \cdot a = g'(L)$. In this case we let $\alpha = \alpha' = \epsilon$.
- If $v \in S \times A$, then let it be (t, b) . We must have $b \in HI$, because by definition of F_{al}^2 , $f(L)$ is in $LO \cup \{\epsilon\}$; if we had $b \in LI$ then $g(L) = o' \cdot b$ with $o' \in LO$, which implies $f(L) \neq g(L)$, a contradiction. Since $b \in HI$, we have $((t, b), g) \xrightarrow{o''} (r, g'')$ with $o'' \in HO$ and $r \in S$. It is not hard to see that $g''(L) = g(L) = f(L)$. Since every action is enabled on r , there exists $(r, g'') \xrightarrow{a} ((r, a), g')$, and it follows $g'(L) = g''(L) \cdot a = f(L) \cdot a = f'(L)$. In this case we let $\alpha = o''$ and $\alpha' = \epsilon$.

Alternately, suppose that $a \in LO$. Then $u \in S \times A$ by the definition of the function F_{al}^2 , so u is in the form of (s, b) with $s \in S$ and $b \in LI$. By the definition of UF_l and F_{al}^2 , we have $f(L)$ in the form of $o \cdot b$ for some $o \in LO$, therefore $g(L) = f(L) = o \cdot b$ and v must be in the form (t, b) since otherwise $f(L) \neq g(L)$. Moreover there exist f'' and g'' such that $(s, f'') \sim' (t, g'')$ with $f''(L) = g''(L) = o$. By Lemma 5.31 there exists $h_1, h_2 \in (O \cup \{\epsilon_0\})^D$ such that $(s, h_1) \sim (t, h_2)$ on $UF(M)$. Then in $UF(M)$ we have $(a, (u', h'_1)) \in next((s, h_1), b)$, and by BNS_a there exists $(a, (v', h'_2)) \in next((t, h_2), b)$ with $h'_1(L) = h'_2(L) = a$. So $(a, v') \in next(t, b)$ in M , hence $(t, b) \xrightarrow{a} v'$ in $F_{al}^2(M)$. Therefore, in $UF^L(F_{al}^2(M))$ we have $(v, g) = ((t, b), g) \xrightarrow{a} (v', g')$ and $g'(L) = a = f'(L)$. Consequently, $(u', f') \sim' (v', g')$, and we have the requirements of W3 with $\alpha = \alpha' = \epsilon$.

For the ‘if’, suppose $UF_l(F_{al}^2(M))$ is in BNS_l^w , we show that the relation \sim defined by $(s, f) \sim (t, g)$ iff $f(L) = g(L)$ on $UF(M)$ is an unwinding relation.

- For LR_a , if $a \in AH$, it follows from the definition of UF that for all $(o, (t, g)) \in next((s, f), a)$ we have $f(L) = g(L)$, hence $(s, f) \sim (t, g)$.
- For SC_a , suppose $a \in AL$ and $(s, f) \sim (t, g)$ and $(o, (s', f')) \in next((s, f), a)$. By Lemma 5.31, there exists reachable states (s, h_1) and (t, h_2) of $UF_l(F_{al}(M))$ such that $(s, h_1) \sim' (t, h_2)$. Moreover, by the construction of $UF_l(F_{al}^2(M))$, there exist transitions $(s, h_1) \xrightarrow{a} ((s, a), h'_1) \xrightarrow{o} (s', h''_1)$. Since \sim' is a weak McCullough unwinding relation, there exist $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in HO^*$ such that $(t, h_2) \xrightarrow{\alpha_1 \cdot a \cdot \alpha_2} ((t, a), h'_2) \xrightarrow{\alpha_3 \cdot o \cdot \alpha_4} (t', h''_2)$ and $(s', h''_1) \sim' (t', h''_2)$, and obviously by the definition of F_{al}^2 we have $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = \epsilon$. This gives us $(o, (t', g')) \in next((t, g), a)$ with $g'(L) = o = f'(L)$. So $(s', f') \sim (t', g')$. \square

In the case of restrictiveness, we found that the two different notions $RES_l \subseteq RES_l^w$ that correspond to RES_a under the mappings F_{al}^1 and F_{al}^2 , respectively, are identical on the range of F_{al}^1 .

While we similarly have that BNS_a corresponds to BNS_l and BNS_l^w under F_{al}^1 and F_{al}^2 , respectively, we note that it can be shown that we have neither $BNS_l \subseteq BNS_l^w$, nor are these notions identical on the range of either F_{al}^1 and F_{al}^2 . However, such a relationship is not necessarily desirable. The intuition for BNS is that it states that, with respect to L , future behaviour is determined by L 's current observation. However, the definitions BNS_l and BNS_l^w are motivated by quite different intuitive interpretations of how the notion of “current observation” is encoded in a labelled transition system.

6. Conclusion

We have studied the relationships between a variety of definitions of noninterference under a number of mappings between different semantic frameworks. The results of the paper are summarised in Fig. 8, which depicts the semantic frameworks we have considered, the mappings between them, and how these mappings relate various definitions of security. In particular, the diagram indicates when notions of security in different semantic frameworks correspond under semantic mappings between these frameworks. Also depicted are several cases where what are generally distinct definitions of security collapse when restricted to the range of these mappings. For the practitioner whose model fits within either the state- or action-observed automaton framework, these collapses provide assurance that classical definitions such as nond-educability, restrictiveness and behavioural nondeterministic security remain of relevance and do not miss issues that have been the topic of the process algebraic studies. Rather, the distinctions between the many new process algebraic definitions arise from subtleties that appear only in the context of the richer expressiveness of the process algebraic semantics.

While there have been a number of extensive comparative studies of definitions of noninterference within semantic frameworks [24,3], work on the comparison of different frameworks has been more limited. Focardi et al. [5] connects language based security with a particular process algebraic property by a one-way translation. Focardi and Gorrieri [3] discuss a number of connections between CCS based and CSP based security properties on non-divergent processes. The first connection is that failure semantics, which is the default semantics of CSP (without divergence), is strictly weaker than bisimulation semantics, so that if the failure based properties (such as FNDC, FSNNI) are defined, they will be strictly weaker than their corresponding bisimulation based properties (such as BNDC, BSNNI) but strictly stronger than their corresponding trace based properties (such as NDC, SNNI). Second, they compared Roscoe's *eager* and *lazy* security properties [20], which are based on low determinism, with the bisimulation based properties on labelled transition systems. It is shown that bisimulation based properties are strictly weaker than the *lazy* security property, but not comparable with the *eager* security property. Connections of the type that we have discussed between unwinding based definitions and bisimulation have also been noted in the context of CSP approaches to security [21]. Mantel and Sabelfeld studied the relationship between programming language security and trace based security in [18], in which a time-sensitive bisimulation based security is connected to a trace based property of [10], by translating a program of a particular language into a state event system. Another work by Morgan links a state based approach to modelling concurrency to an event based approach (CSP), by expressing traces, failures and divergences of CSP as weakest precondition formulas over action systems [17], but without considering security.

We have focused in our work on mappings from state based models, in order to create a bridge from this type of model (which, for pragmatic reasons, is still the most commonly used approach in applied work on formal verification

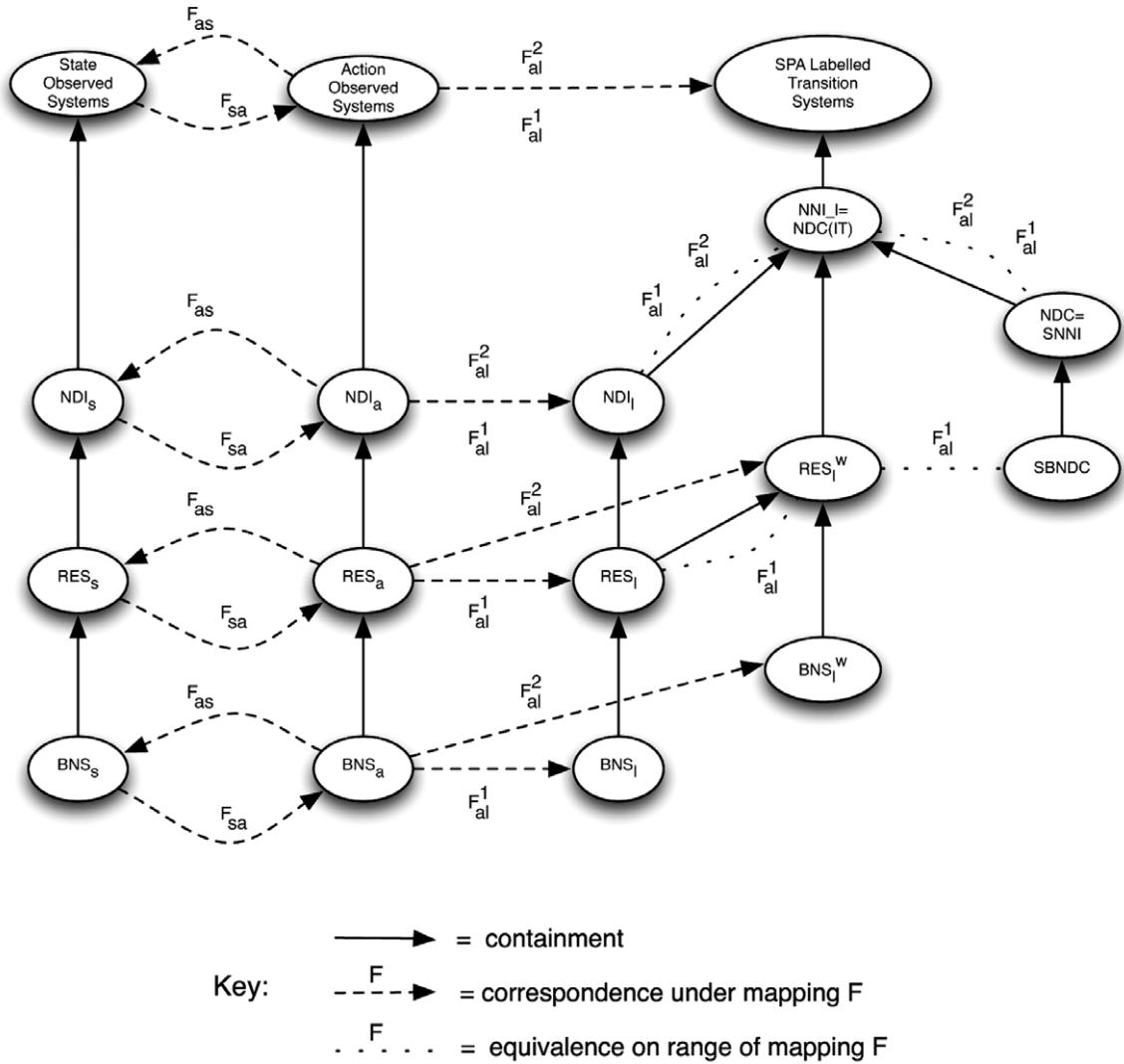


Fig. 8. Relationships between properties under transformations.

of information flow properties in operating systems [27,8,19]) to the more recent literature on security in process algebraic settings. Our results show that similar properties in different models do often correspond in a precise sense, but highlight some subtleties. We found that the most direct correspondence between existing notions on the various models is obtained when the obligatory observations in the state-observed model are treated as optional when mapped to the other models. However, for another translation, that treats observations as obligatory, we were able to give a new definition of unwinding that leads to a correspondence of all the notions we consider under this translation.

Also, and of particular interest, given our motivation from operating systems verification, the strongest process algebraic notion, $SBNDC$, is logically weaker on the automaton models than the notion BNS_s which seems closest to the models and properties used in the operating systems verification literature [8,19]. Even if one considers a logically weaker notion to capture one's intuitions for security, there is no harm in proving a stronger property (and there is a benefit if it yields a simpler proof). Therefore, although BNS has been neglected in the recent theoretical literature, we believe that it remains of relevance.

Our focus in this paper, following much of the literature, has been on asynchronous models and the specific policy $L \leq H$. However, the operating systems literature that originally motivated the study of noninterference also involves issues such as separation policy, intransitive noninterference, scheduling and synchrony that go beyond the concerns we have treated in this paper. We intend to address these issues in future work.

Appendix

This Appendix contains the proofs of some lemmas presented in the article.

Proof (Theorem 3.7). A proof for the action-observed system can be found in [23]. For state-observed systems, the proof is similar to [23].

(1) Suppose there exists an unwinding relation \sim_L satisfying Output Consistency_s, Locally Respects and Step Consistency. We show that $s_0 \circ \alpha \sim_L s_0 \circ \text{purge}_L(\alpha)$ for all $\alpha \in A^*$. It follows from this that $\text{obs}_L(s_0 \circ \alpha) = \text{obs}_L(s_0 \circ \text{purge}_L(\alpha))$, by Output Consistency_s, so $M \in NI_s$. We proceed by induction on length of α . For the base case $\alpha = \epsilon$, we have $\epsilon = \text{purge}_L(\epsilon)$, so $s_0 \circ \epsilon \sim_L s_0 \circ \text{purge}_L(\epsilon)$, since \sim_L is reflexive. Suppose $s_0 \circ \alpha \sim_L s_0 \circ \text{purge}_L(\alpha)$ for some α . We show the case for $\alpha \cdot a$ with $a \in A$.

- If $\text{dom}(a) = H$, then $\text{purge}_L(\alpha \cdot a) = \text{purge}_L(\alpha)$, and $s_0 \circ \alpha \sim_L \text{step}(s_0 \circ \alpha, a) = s_0 \circ (\alpha \cdot a)$ by Locally Respects. Since $s_0 \circ \alpha \sim_L s_0 \circ \text{purge}_L(\alpha)$ by induction hypothesis, we obtain by the fact that \sim_L is an equivalence relation that $s_0 \circ (\alpha \cdot a) \sim_L s_0 \circ \text{purge}_L(\alpha) = s_0 \circ \text{purge}_L(\alpha \cdot a)$.
- If $\text{dom}(a) = L$, then $\text{purge}_L(\alpha \cdot a) = \text{purge}_L(\alpha) \cdot a$. Since $s_0 \circ \alpha \sim_L s_0 \circ \text{purge}_L(\alpha)$ by induction hypothesis, we have $\text{step}(s_0 \circ \alpha, a) \sim_L \text{step}(s_0 \circ \text{purge}_L(\alpha), a)$ by Step Consistency, i.e., $s_0 \circ (\alpha \cdot a) \sim_L s_0 \circ (\text{purge}(\alpha) \cdot a) = s_0 \circ \text{purge}_L(\alpha \cdot a)$.

(2) Suppose that a deterministic state-observed system M is in NI_s , i.e., $\text{obs}_L(s_0 \circ \alpha) = \text{obs}_L(s_0 \circ \text{purge}_L(\alpha))$ for all $\alpha \in A^*$.

We show that there exists an unwinding relation on M . Similar to [23], let $\overset{L}{\sim}$ be the relation such that $s \overset{L}{\sim} t$ if for all $\alpha \in A^*$, $\text{obs}_L(s \circ \alpha) = \text{obs}_L(t \circ \alpha)$. We show that $\overset{L}{\sim}$ satisfies Output Consistency_s, Locally Respects and Step Consistency.

- For Output Consistency_s, if $s \overset{L}{\sim} t$ we have $\text{obs}_L(s \circ \epsilon) = \text{obs}_L(t \circ \text{purge}_L(\epsilon))$, which is just $\text{obs}_L(s) = \text{obs}_L(t)$.
- For Locally Respects, suppose there exists $s \in S$ and $a \in A_H$ such that $s \not\overset{L}{\sim} \text{step}(s, a)$. Then there exists $\alpha \in A^*$ such that $\text{obs}_L(s \circ \alpha) \neq \text{obs}_L(s \circ (a \cdot \alpha))$. Since s is reachable there is $\alpha' \in A^*$ such that $s = s_0 \circ \alpha'$. Therefore $\text{obs}_L(s_0 \circ (\alpha' \cdot a \cdot \alpha)) \neq \text{obs}_L(s_0 \circ (\alpha' \cdot \alpha))$. However $\text{purge}_L(\alpha' \cdot a \cdot \alpha) = \text{purge}_L(\alpha' \cdot \alpha)$ by $a \in A_H$, so $\text{obs}_L(s_0 \circ (\alpha' \cdot a \cdot \alpha)) = \text{obs}_L(s_0 \circ (\alpha' \cdot \alpha))$ by the system in NI_s , which is a contradiction.
- For Step Consistency, suppose there exists $s, t \in S$ and $a \in A$ such that $s \overset{L}{\sim} t$ and $\text{step}(s, a) \not\overset{L}{\sim} \text{step}(t, a)$. Then there exists $\alpha \in A^*$ such that $\text{obs}_L(\text{step}(s, a) \circ \alpha) \neq \text{obs}_L(\text{step}(t, a) \circ \alpha)$, i.e., $\text{obs}_L(s \circ (a \cdot \alpha)) \neq \text{obs}_L(t \circ (a \cdot \alpha))$, contradicting $s \overset{L}{\sim} t$. \square

Proof (Lemma 3.11). It suffices to show that if $M_1 \approx M_2$ and $M_1 \in RES_a$ then $M_2 \in RES_a$. Since $M_1 \in RES_a$, there exists an unwinding relation \sim_1 on S_1 satisfying SC_a and LR_a . Define \sim_2 on S_2 by $t_1 \sim_2 t_2$ if there exists $s_1, s_2 \in S_1$ such that $s_1 \sim_1 s_2$, $s_1 \approx t_1$ and $s_2 \approx t_2$. To show that \sim_2 is reflexive, for every reachable $t \in S_2$, we have a run starting from s_0^2 to t . By $s_0^1 \approx s_0^2$, an induction on this run leads us to a state $s \in S_1$ with $s \approx t$. Then $t \sim_2 t$ is by $s \sim_1 s$. \sim_2 is both symmetric and transitive since \sim_1 is symmetric and transitive. It is straightforward to show that \sim_2 is an unwinding relation on S_2 .

- To show SC_a , let $t_1 \sim_2 t_2$ and $(o, t'_1) \in \text{next}_2(t_1, a)$ for some $a \in A_L$. By definition there exist $s_1, s_2 \in S_1$ such that $s_1 \sim_1 s_2$, $s_1 \approx t_1$ and $s_2 \approx t_2$. Then there exists $(o, s'_1) \in \text{next}_1(s_1, a)$ such that $s'_1 \approx t'_1$. From $s_1 \sim_1 s_2$ there exists $(o, s'_2) \in \text{next}_1(s_2, a)$ such that $s'_1 \sim_1 s'_2$. Then from bisimulation there exists $(o, t'_2) \in \text{next}_2(t_2, a)$ such that $s'_2 \approx t'_2$, and we have all that is required to establish $t'_1 \sim_2 t'_2$.
- To show LR_a , for any reachable state $t \in S_2$, there exists a sequence of transitions from s_0^2 to t . From $s_0^1 \approx s_0^2$, we prove by induction that there exists a sequence of transitions from s_0^1 to a state $s \in S_1$ and $s \approx t$. Then for all $a \in A_H$ with $(o, t') \in \text{next}(t, a)$, there exists $(o, s') \in \text{next}(s, a)$ such that $s' \approx t'$. From \sim_1 satisfying LR_a we have $s \sim_1 s'$. This gives the result $t \sim_2 t'$ as required. \square

Proof (Lemma 5.25). Since a McCullough unwinding relation is also a weak McCullough unwinding relation by Lemma 5.19, we only need to show that if there is a weak McCullough unwinding relation on M then there is an unwinding relation on M . Let \sim be a weak McCullough unwinding relation. We show that \sim is also a McCullough unwinding relation. Let $s \sim t$.

- (M1) For all $\alpha, \alpha' \in I^*$ satisfying $\alpha|L = \alpha'|L$ and $s \xrightarrow{\alpha} s'$, let $\alpha = \alpha_0 a_0 \alpha_1 a_1 \dots a_{n-1} \alpha_n$, and $\alpha' = \alpha'_0 a_0 \alpha'_1 a_1 \dots a_{n-1} \alpha'_n$, where $a_i \in LI$ for $i = 0, \dots, n-1$ and $\alpha_i, \alpha'_i \in HI^*$ for $i = 0, \dots, n$. We also assume there are intermediate states $s_0, s_1 \dots s_n$ such that $s_i \xrightarrow{\alpha_i a_i} s_{i+1}$ for all i , and $s = s_0$, and $s_n \xrightarrow{\alpha_n} s'$. We prove by induction that there exist states $t_0, t_1 \dots t_n$ such that $t_i \xrightarrow{\alpha'_i a_i} t_{i+1}$ and $s_i \sim t_i$ for all i . The base case is trivial. Suppose $s_k \sim t_k$ and $s_k \xrightarrow{\alpha_k} s'_k \xrightarrow{a_k} s_{k+1}$. By W1, $s_k \sim s'_k$, therefore $t_k \sim s'_k$. Also, for each sequence α'_k , by High input-totality, there exists t'_k such that $t_k \xrightarrow{\alpha'_k} t'_k$, and by W1 we have $t_k \sim t'_k$. Thus $s'_k \sim t'_k$. From $s'_k \xrightarrow{a_k} s_{k+1}$, by W3, there exist $t'_k \xrightarrow{\gamma \cdot a_k \cdot \gamma'} t_{k+1}$ and $s_{k+1} \sim t_{k+1}$ with $\gamma, \gamma' \in HO^*$. By the fact that every output transition goes to its source state, we have $t'_k \xrightarrow{a_k} t_{k+1}$. For the final case which is $s_n \sim t_n$ and $s_n \xrightarrow{\alpha_n} s'$ implies there exist t' and $\alpha'_n \in HO^*$ such that $t_n \xrightarrow{\alpha'_n} t'$ and $s' \sim t'$, this can be shown in a similar way.
- (M2) For all $\alpha \in O^*$, $s \xrightarrow{\alpha} s'$ implies $s = s'$. We take $\alpha' = \epsilon$ and $t' = t$, so that $t \xrightarrow{\alpha'} t'$ and $s' = s \sim t = t'$. \square

Proof (Lemma 5.26). For the ‘if’ direction it is obvious that \approx is a weak McCullough unwinding relation. For the ‘only if’, suppose $F_{al}^2(M) \in RES_l^w$. Then there is a weak McCullough unwinding relation \sim on $F_{al}^2(M)$. We show that \sim satisfies the conditions on \approx . Let S be the set of states of M .

(W1') For $a \in HI$, W1' is immediate from W1. For $o \in HO$, note that if $x \xrightarrow{o} t$ then $x = (s, a)$ for some $a \in HI$ and $s \in S$ and $t \in S$. By W1 and symmetry, $(s, a) \sim s$, so by W2 there exist $\alpha \in HO^*$ and a state s' such that $s \xrightarrow{\alpha} s'$ and $t \sim s'$. However, no actions in HO are enabled at s , which means that the only possibility is $\alpha = \epsilon$ and we get $t \sim s' = s$. So $x = (s, a) \sim t$ by the fact that \sim is an equivalence relation.

(W2') Suppose $s \sim t$ and $s \xrightarrow{a} s'$ for $a \in L$. By W3, there exist $\beta, \beta' \in HO^*$ and a state t' such that $t \xrightarrow{\beta \cdot a \cdot \beta'} t'$ and $s' \sim t'$. We need to find $\alpha \in HO^*$ and a state y such that $t \xrightarrow{\alpha \cdot a} y$ and $s' \sim y$. We consider the cases of $a \in LI$ and $a \in LO$ separately. If $a \in LI$, then we must have $s \in S$ and $s' = (s, a)$. We consider two cases, depending on whether $t \in S$.

- If $t \in S$, then actions in HO are enabled neither at t , nor at (t, a) . Therefore, we must have $\beta = \beta' = \epsilon$, and $t' = (t, a)$, so $t \xrightarrow{a} (t, a) = t'$. Here we take $\alpha = \epsilon$ and $y = t' \sim s'$.
- If t is of the form (r, b) with $r \in S$, it is impossible that $b \in A_L$ because in this case no outputs in HO or inputs in LI would be enabled at (r, b) . Thus $b \in A_H$ and $t = (r, b) \xrightarrow{o} r' \xrightarrow{a} (r', a)$ for some $r' \in S$ and $o \in HO$. Indeed, we must have $\beta = o$ and $\beta' = \epsilon$ (since no HO event can be enabled at (r', a)). Thus, $(r', a) \sim s'$, and we may take $\alpha = o$ and $y = (r', a)$.

Suppose that $a \in LO$. By W3, there exist $\beta, \beta' \in HO^*$ such that $t \xrightarrow{\beta \cdot a \cdot \beta'} t'$ and $s' \sim t'$. Since there are no successive output transitions in $F_{al}^2(M)$, we must have $\beta = \beta' = \epsilon$, so $t \xrightarrow{a} t'$. Thus, we may take $\alpha = \epsilon$ and $y = t'$. \square

References

- [1] W.R. Bevier, W.D. Young, A state-based approach to noninterference, in: Proc. IEEE Computer Security Foundations Workshop, 1994, pp. 11–21.
- [2] R. Focardi, R. Gorrieri, A classification of security properties for process algebras, Journal of Computer Security 1 (1995) 5–33.
- [3] R. Focardi, R. Gorrieri, Classification of security properties, in: FOSAD 2000, in: LNCS, vol. 2171, 2001, pp. 331–396.
- [4] R. Forster, Non-interference properties for nondeterministic processes. Ph.D. Thesis, Dissertation for transfer to D.Phil status, Oxford University Computing Laboratory, 1997.
- [5] R. Focardi, S. Rossi, A. Sabelfeld, Bridging language-based and process calculi security, in: Proc. Foundations of Software Science and Computation Structures, FoSSaCS, in: LNCS, vol. 3441, 2005, pp. 299–315.
- [6] J.A. Goguen, J. Meseguer, Security policies and security models, in: IEEE Symposium on Security and Privacy, April 1982, pp. 11–20.
- [7] J.A. Goguen, J. Meseguer, Unwinding and inference control, in: IEEE Symposium on Security and Privacy, 1984, p. 75.
- [8] D. Greve, M. Wilding, W.M. van Fleet, A separation kernel formal security policy, in: ACL2 Workshop, 2003.
<http://www.cs.utexas.edu/users/moore/ac12/workshop-2003>.
- [9] C.A.R. Hoare, Communicating Sequential Processes, Prentice Hall, 1985.
- [10] H. Mantel, Possibilistic definitions of security – an assembly kit, in: 13th IEEE Computer Security Foundations Workshop, July 2000, pp. 185–199.
- [11] D. McCullough, Specifications for multi-level security and a hook-up property, in: Proc. IEEE Symposium on Security and Privacy, 1987, pp. 161–166.
- [12] D. McCullough, Noninterference and the compositability of security properties, in: Proc. IEEE Symposium on Security and Privacy, 1988, pp. 177–186.
- [13] D. McCullough, A hookup theorem for multi-level security, IEEE Transactions on Software Engineering 16 (6) (1990) 563–568.
- [14] J. McLean, A general theory of composition for trace sets closed under selective interleaving functions, in: Proc. IEEE Symposium on Security and Privacy, May 1994, pp. 79–93.
- [15] R. Milner, Communication and Concurrency, Prentice-Hall, 1989.
- [16] J.K. Millen, Hookup security for synchronour machine, in: Proc. IEEE Computer Security Foundations Workshop, 1990, pp. 84–90.
- [17] C.C. Morgan, Of wp and CSP, in: Beauty is Our Business: A Birthday Salute to Edsger W. Dijkstra, Springer-Verlag, 1990, pp. 319–326.
- [18] H. Mantel, A. Sabelfeld, A unifying approach to the security of distributed and multi-threaded programs, Journal of Computer Security 4 (2003) 615–676.
- [19] W. Martin, P. White, F.S. Taylor, A. Goldberg, Formal construction of the mathematically analyzed separation kernel, in: Proc. 15th IEEE Int. Conf. on Automated Software Engineering, ASE'00, 2000.
- [20] A.W. Roscoe, CSP and determinism in security modelling, in: Proc. IEEE Symposium on Security and Privacy, 1995, pp. 114–221.
- [21] P.Y.A. Ryan, S.A. Schneider, Process algebra and non-interference, Journal of Computer Security 1–2 (2001) 75–103.
- [22] J. Rushby, Proof of separability a verification technique for a class of security kernels, in: Proc. 5th International Symposium on Programming, Turin, Italy, April 1982, pp. 352–367.
- [23] J. Rushby, Noninterference, transitivity, and channel-control security policies, Technical Report, SRI international, Dec. 1992.
- [24] P.Y.A. Ryan, Mathematical models of computer security, in: FOSAD 2000, in: LNCS, vol. 2171, 2001, pp. 1–62.
- [25] D. Sutherland, A model of information, in: Proc. National Computer Security Conference, 1986, pp. 175–183.
- [26] R. van der Meyden, What, indeed, is intransitive noninterference? (extended abstract), in: Proc. European Symposium on Research in Computer Security, in: LNCS, vol. 4734, Springer, 2007, pp. 235–250.
- [27] D. von Oheimb, Information flow control revisited: Noninfluence = Noninterference + Nonleakage, in: Proc. European Symposium on Research in Computer Security, ESORICS 2004, in: LNCS, vol. 3193, Springer, 2004, pp. 225–243.
- [28] J.T. Wittbold, D.M. Johnson, Information flow in nondeterministic systems, in: Proc. IEEE Symposium on Security and Privacy, 1990, pp. 144–161.
- [29] A. Zakinthinos, E.S. Lee, A general theory of security properties, in: Proc. IEEE Symposium on Security and Privacy, May 1997, pp. 94–102.