What, Indeed, is Intransitive Noninterference?*

Ron van der Meyden

School of Computer Science and Engineering,
University of New South Wales
meyden@cse.unsw.edu.au

Abstract. This paper argues that Haigh and Young's definition of noninterference for intransitive security policies admits information flows that are not in accordance with the intuitions it seeks to formalise. Several alternative definitions are discussed, which are shown to be equivalent to the classical definition of noninterference with respect to transitive policies. Rushby's unwinding conditions for intransitive noninterference are shown to be sound and complete for one of these definitions, TA-security. Access control systems compatible with a policy are shown to be TA-secure, and it is also shown that TA-security implies that the system can be interpreted as an access control system.

1 Introduction

The term 'noninterference' is used in the computer security literature to refer to formal definitions of information flow or causality between security domains. The classical theory of noninterference [GM82] dealt with transitive policies, which are closely related to partially ordered security levels. This theory is unable to deal with certain systems requiring channel control and downgrading [Rus81]. To overcome these limitations, Haigh and Young [HY87] proposed a variant of the classical definition for channel control applications, which was further promulgated by Rushby [Rus92] for intransitive policies more generally. Roscoe and Goldsmith [RG99] have argued that the variant definition is in fact inadequate for dealing with downgrading, and have proposed an alternate definition. Their arguments do not seem to have been universally accepted, however, and the Haigh and Young definition remains in use and continues to be the subject of research [HALL$^+$05,MS04,Ohe04].

In this paper, we present a new argument against this definition, showing that it is too weak for the intuitions it seeks to capture. We present an example that shows that it allows information to flow to an agent, that could not have come from the agents from which it is permitted to acquire information.

This leads us to consider alternative definitions. We show that there is in fact a spectrum of different definitions of noninterference for possibly intransitive

---

* Version of January 3, 2008. Thanks to the Courant Institute, New York University, for hosting a sabbatical visit during which this research was conducted. Work of the author supported by an Australian Research Council Discovery grant.

policies, all having some intuitive plausibility, and all equivalent to the classical definition in the case of transitive policies. The weakest of these definitions is the classical purge-based definition, the strongest is Haigh and Young's definition. We define several notions of intermediate strength. These definitions state that the agent should not have more information than the maximal amount it is permitted to have. This maximal amount of information is modelled by viewing actions as transmitting information. The notions differ in the information that may be transmitted by an action. One of these notions, TO-security, states that an agent may not transmit information that it has not directly observed. Another other notion, TA-security, takes a more liberal view, in which an agent's actions may transmit information about previous actions that it is permitted to have, even if it has not actually observed this information. A third notion, ITO-security, is similar, but allows for a faster transmission of information in that it permits an agent to transmit information by means of the same action by which it acquires that information.

We then study these new definitions from the point of view of proof techniques and an application that have been held in the literature to be of significance for intransitive noninterference. We begin with a discussion of "unwinding conditions," which provide a proof technique for noninterference, but can be taken as a definition of security in their own right. Rushby proved that the classical unwinding conditions of Goguen and Meseguer provide a complete proof technique for noninterference in the transitive case. He proposes a weakening of these conditions for intransitive policies (correcting an earlier proposal by Haigh and Young [HY87]). He establishes soundness of the weakened unwinding conditions, but not completeness. We give an explanation of this: Rushby's conditions are not complete for the Haigh and Young definition of noninterference. Instead, they are sound and complete for the stronger notion of TA-security. There is a somewhat surprising subtlety in this statement: for completeness, the weakened unwinding conditions must be applied to the appropriate bisimilar system, but the existence of the weak unwindings is not preserved under bisimulation.

We also follow Rushby in considering the behaviour of the definitions on access control systems, the class of applications originally motivating the literature on noninterference. Rushby showed that access control systems satisfying a condition of structural consistency with a policy satisfy Haigh and Young's definition of intransitive noninterference. We argue that Rushby's definition of access control systems can be weakened, and that access control systems consistent with a policy satisfy the stronger notion of TA-security as well as Haigh and Young's definition of security. Moreover, we also show that TA-security implies that there is a way to interpret the system as an access control system in the weakened sense. This shows that TA-security is in some sense equivalent to the existence of an access control implementation of the system.

These results provide strong evidence that TA-security, rather than Haigh and Young's definition, best fits the original objectives for the notion of intransitive noninterference. Nevertheless, the stronger notion of TO-security may well be equally significant for practical purposes. As evidence of this, we prove that access control systems structurally consistent with a policy also satisfy the stronger notion of TO-security, provided we work with an appropriate notion of observation for such systems.

The structure of the paper is as follows. Section 2 recalls the Haigh and Young definition, and presents our new argument against the definition. In Section 3 we introduce some new definitions of noninterference for intransitive noninterference, and show how they are related. We discuss unwinding conditions in Section 4. The results on access control systems are presented in Section 5. We close in Section 6 with some remarks concerning related research and issues requiring investigation.

2 Intransitive Noninterference

The notion of *noninterference* was first proposed by Goguen and Meseguer [GM82]. Early work on this area was motivated by multi-level secure systems, and dealt with deterministic systems and partially ordered (hence transitive) information flow policies. A significant body of work has developed since then, with a particular focus on generalization to the case of nondeterministic systems [Sut86,WJ90,McC88,FG01,Rya01] and intransitive policies [Rus92,RG99,Ohe04]. We focus in this paper on intransitive policies in the deterministic case.

Several different types of semantic models have been used in the literature on noninterference. (See [MZ06] for a comparison and a discussion of their relationships.) We work here with the state-observed machine model used by Rushby [Rus92], but similar results can be obtained for other models. [1] This model consists of deterministic machines of the form $\langle S, s_0, A, \mathtt{step}, \mathtt{obs}, \mathtt{dom}\rangle$, where S is a set of states, $s_0 \in S$ is the *initial state*, A is a set of actions, $\mathtt{dom} : A \rightarrow D$ associates each action to an element of the set D of security domains, $\mathtt{step} : S \times A \rightarrow S$ is a deterministic transition function, and $\mathtt{obs} : S \times D \rightarrow O$ maps states to an observation in some set O, for each security domain. We may also refer to security domains more succinctly as "agents". We write $s \cdot \alpha$ for the state reached by performing the sequence of actions $\alpha \in \mathit{Actions}^*$ from state s, defined inductively by $s \cdot \epsilon = s$, and $s \cdot \alpha a = \mathtt{step}(s \cdot \alpha, a)$ for $\alpha \in A^*$ and $a \in A$. Here ϵ denotes the empty sequence.

Noninterference policies, as they are now usually presented[2], are relations $\rightarrowtail \subseteq D \times D$, with $u \rightarrowtail v$ intuitively meaning that "actions of domain u are permitted to interfere with domain v", or "information is permitted to flow from domain u to domain v". Since, intuitively, a domain should be allowed to interfere with, or have information about, itself, this relation is assumed to be reflexive. In early work on noninterference, it is also assumed to be transitive.

[1] In a companion paper [Mey07a] we also treat Rushby's action-observed model, and show that the corresponding definitions in that model are related to those in the state-observed model by means of a natural mapping from action observed systems to state-observed systems.

[2] Goguen and Meseguer used a slightly richer notion.

Noninterference is given a formal semantics in the transitive case using a definition based on a "purge" function [GM82]. Given a set $E \subseteq D$ of domains and a sequence $\alpha \in A^*$, we write $\alpha \upharpoonright E$ for the subsequence of all actions a in α with $\mathtt{dom}(a) \in E$. Given a policy $\rightarrowtail$, we define the function $\mathtt{purge} : A^* \times D \rightarrow A^*$ by

$$\mathtt{purge}(\alpha, u) = \alpha \upharpoonright \{v \in D \mid v \rightarrowtail u\}.$$

(For clarity, we may use subscripting of agent arguments of functions, writing e.g., $\mathtt{purge}(\alpha, u)$ as $\mathtt{purge}_u(\alpha)$.) The system M is said to be *secure with respect to the transitive policy* $\rightarrowtail$ when for all $\alpha \in A^*$ and domains $u \in D$, we have $\mathtt{obs}_u(s_0 \cdot \alpha) = \mathtt{obs}_u(s_0 \cdot \mathtt{purge}_u(\alpha))$. That is, each agent's observations are as if only interfering actions had been performed. An equivalent formulation (which we state more generally for policies that are not necessarily transitive, in anticipation of later discussion) is the following:

Definition 1. *A system M is* P-secure *with respect to a policy $\rightarrowtail$ if for all sequences $\alpha, \alpha' \in A^*$ such that $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\alpha')$, we have $\mathtt{obs}_u(s_0 \cdot \alpha) = \mathtt{obs}_u(s_0 \cdot \alpha')$.*

This can be understood as saying that agent u's observation depends only on the sequence of interfering actions that have been performed.

Haigh and Young [HY87] generalised the definition of the purge function to intransitive policies as follows. Intuitively, the intransitive purge of a sequence of actions with respect to a domain u is the largest subsequence of actions that could form part of a causal chain of effects (permitted by the policy) ending with an effect on domain u. More formally, the definition makes use of a function $\mathtt{sources} : A^* \times D \Rightarrow \mathcal{P}(D)$ defined inductively by $\mathtt{sources}(\epsilon, u) = \{u\}$ and

$$\mathtt{sources}(a\alpha, u) = \mathtt{sources}(\alpha, u) \cup \{\mathtt{dom}(a) \mid \exists v \in \mathtt{sources}(\alpha, u)(\mathtt{dom}(a) \rightarrowtail v)\}$$

for $a \in A$ and $\alpha \in A^*$. Intuitively, $\mathtt{sources}(\alpha, u)$ is the set of domains v such that there exists a sequence of permitted interferences from v to u within α. The *intransitive purge* function $\mathtt{ipurge} : A^* \times D \rightarrow A^*$ is then defined inductively by $\mathtt{ipurge}(\epsilon, u) = \epsilon$ and

$$\mathtt{ipurge}(a\alpha, u) = \begin{cases} a \cdot \mathtt{ipurge}(\alpha, u) & \text{if } \mathtt{dom}(a) \in \mathtt{sources}(a\alpha, u) \\ \mathtt{ipurge}(\alpha, u) & \text{otherwise} \end{cases}$$

for $a \in A$ and $\alpha \in A^*$. An alternative, equivalent formulation that we will find useful is the following: given a set $X \subseteq D$, define $\mathtt{ipurge}_X(\alpha)$ inductively by $\mathtt{ipurge}_X(\epsilon) = \epsilon$ and

$$\mathtt{ipurge}_X(\alpha a) = \begin{cases} \mathtt{ipurge}_{X \cup \{\mathtt{dom}(a)\}}(\alpha) \cdot a & \text{if } \mathtt{dom}(a) \rightarrowtail u \in X \\ \mathtt{ipurge}_X(\alpha) & \text{otherwise} \end{cases}$$

Then $\mathtt{ipurge}_u(\alpha)$ is identical to $\mathtt{ipurge}_{\{u\}}(\alpha)$. Haigh and Young's definition of security uses the intransitive purge function in place of the purge function in Goguen and Meseguer's definition: M is secure with respect to a policy $\rightarrowtail$

if for all sequences $\alpha \in A^*$, and $u \in D$, we have $\texttt{obs}_u(s_0 \cdot \alpha) = \texttt{obs}_u(s_0 \cdot \texttt{ipurge}_u(\alpha))$. Since the function $\texttt{ipurge}_u$ on A^* is idempotent, this definition, like the definition for the transitive case, can be equivalently formulated as:

Definition 2. *A system M is IP-secure with respect to a (possibly intransitive) policy $\rightarrowtail$ if for all $u \in D$ and all sequences $\alpha, \alpha' \in A^*$ with $\texttt{ipurge}_u(\alpha) = \texttt{ipurge}_u(\alpha')$, we have $\texttt{obs}_u(s_0 \cdot \alpha) = \texttt{obs}_u(s_0 \cdot \alpha')$.*

It can be seen that $\texttt{ipurge}_u(\alpha) = \texttt{purge}_u(\alpha)$ when $\rightarrowtail$ is transitive, so IP-security is in fact a generalisation of the definition of security for transitive policies.

Roscoe and Goldsmith [RG99] (henceforth, RG) have argued that the Haigh and Young definition is incorrect. They present a number of concrete examples to make this case, including a policy $H \rightarrowtail D \rightarrowtail L$, intended to represent that D is a "downgrader" process that decides which of the High (H) secrets may safely be revealed to a Low process L. The essence of their argument is that the definition has the effect that a downgrader D's action permits *all* information about preceding H actions to become known to L, even if the intent of the downgrading action was to release only some specific information about the preceding H actions.

That is, this definition does not enable the intent of specific downgrading actions to be specified. But it might be countered in that intransitive noninterference was not intended to make such fine grained distinctions, but only to express some coarse architectural constraints on information flow. In RG's examples, the information released to L is information that was known to D at the time of release. One might sensibly hold the view that therefore RG's examples are not counterexamples to the intuitive reading of the policy. Indeed, RG's arguments have not been universally accepted as compelling (see, e.g., [Ohe04]).

Nevertheless, we believe that a case can be made that IP-security is too weak, but on different grounds. Note that the intransitive purge $\texttt{ipurge}_u(\alpha)$ preserves not just certain actions from the sequence α, but also their *order*. We claim that this allows u to "know" this order in situations where an intuitive reading of the policy would suggest that it ought not to know this order.

To give precise content to this claim, we introduce some notation from the literature on modal logics of knowledge [FHMV95]. Let *Prop* be a set of atomic propositions. We define a propositional modal logic, with formulas defined as follows: if $p \in \mathit{Prop}$ then p is formula, and if ϕ and ψ are formulas and $u \in D$ is an agent and $G \subseteq D$ is a nonempty set of agents then $\neg\phi$, $\phi \vee \psi$ and $\texttt{K}_u\phi$ and $\texttt{D}_G\phi$ are formulas. We use standard boolean abbreviations such as $\phi \Rightarrow \psi$ for $\neg\phi \vee \psi$. Intuitively, the formula $\texttt{K}_u\phi$ expresses that agent u knows ϕ, and $\texttt{D}_G\phi$ expresses that ϕ is *distributed kowledge* to the group G, which means that the group G, collectively, knows ϕ.

We take the atomic propositions to be interpreted over sequences of actions of a system M with actions A, by means of an interpretation function $\pi : \mathit{Prop} \rightarrow \mathcal{P}(A^*)$. Formulas ϕ are then interpreted as being satisfied at a sequence of actions $\alpha \in A^*$ by means of a relation $M, \pi, \alpha \models \phi$. For atomic propositions $p \in \mathit{Prop}$, this relation is defined by $M, \pi, \alpha \models p$ if $\alpha \in \pi(p)$.

The semantics of the operators for knowledge are given formal meaning using the following notion of *view*. The definition uses an absorbtive concatenation function $\circ$, defined over a set X by, for $s \in X^*$ and $x \in X$, by $s \circ x = s$ if x is equal to the final element of s (if any), and $s \circ x = s\,x$ (ordinary concatenation) otherwise. Define the view of domain u with respect to a sequence $\alpha \in A^*$ using the function $\mathtt{view}_u : A^* \to (A \cup O)^*$ (where O is the set of observations in the system) defined by

$$\mathtt{view}_u(\epsilon) = \mathtt{obs}_u(s_0), \text{ and}$$
$$\mathtt{view}_u(\alpha a) = \begin{cases} \mathtt{view}_u(\alpha)\, a\, \mathtt{obs}_u(s_0 \cdot \alpha) & \text{if } \mathtt{dom}(a) = u, \\ \mathtt{view}_u(\alpha) \circ \mathtt{obs}_u(s_0 \cdot \alpha) & \text{otherwise} \end{cases}$$

That is, $\mathtt{view}_u(\alpha)$ is the sequence of all observations and actions of domain u in the run generated by α, compressed by the elimination of stuttering observations. Intuitively, $\mathtt{view}_u(\alpha)$ is the complete record of information available to agent u in the run generated by the sequence of actions α. The reason we apply the absorbtive concatenation is to capture that the system is asynchronous, with agents not having access to a global clock. Thus, two periods of different length during which a particular observation obtains are not distinguishable to the agent.

Using the notion of view, we may define for each agent u an equivalence relation $\equiv_u$ on sequences of actions by $\alpha \equiv_u \alpha'$ if $\mathtt{view}_u(\alpha) = \mathtt{view}_u(\alpha')$. The semantics for the knowledge operators may then be given by

$$M, \pi, \alpha \models \mathtt{K}_u\phi \text{ if } M, \pi, \alpha' \models \phi \text{ for all sequences } \alpha' \text{ such that } \alpha \equiv_u \alpha'.$$

This is essentially the definition of knowledge used in the literature on reasoning about knowledge [FHMV95] for an agent with *asynchronous perfect recall*.

The notion of distributed knowledge is defined in the literature as follows. First, define the relations $\equiv_G$ on sequences of actions by $\alpha \equiv_G \alpha'$ if $\alpha \equiv_u \alpha'$ for all $u \in G$. The operators $\mathtt{D}_G$ are then given semantics by the clause

$$M, \pi, \alpha \models \mathtt{D}_G\phi \text{ if } M, \pi, \alpha' \models \phi \text{ for all sequences } \alpha' \text{ such that } \alpha \equiv_G \alpha'.$$

Intuitively, this definition says that a fact is *distributed knowledge* to the set of agents G if it could be deduced after combining all the information that these agents have.

We may now present our example illustrating a weakness of IP-security. The essence of the example is that IP-security is consistent with an agent acquiring information that is not distributed knowledge to the agents from which it permitted (by an intransitive policy) to acquire information.

Example 1. Consider the intransitive policy $\rightarrowtail$ given by $H_1 \rightarrowtail D_1$, $H_2 \rightarrowtail D_2$, $D_1 \rightarrowtail L$ and $D_2 \rightarrowtail L$. Intuitively, H_1, H_2 are two High security domains, D_1, D_2 are two downgraders, and L is an aggregator of downgraded information. For this policy, channel control, one of the motivations for intransitive noninterference, would require that any information about L_1 and L_2 available to L must have reached L via the downgraders D_1 and D_2. We may capture this intuition more formally by expecting that if M is a system that is secure with respect to this policy and π interprets the atomic proposition p as expressing some property depending only on the behaviour of H_1 and H_2, then we should have

$$M, \pi, \alpha \models \mathtt{K}_L p \Rightarrow \mathtt{D}_{\{D_1,D_2\}} p \tag{1}$$

for all $\alpha \in A^*$. That is, if a fact about H_1, H_2 is known to L, then it should be distributed knowledge to D_1, D_2. We show that if security is interpreted as $IP - security$, then this expectation can be false.

Define the system M with actions $A = \{h_1, h_2, d_1, d_2, l\}$ with domains H_1, H_2, D_1, D_2, and L, respectively. The set of states of M is the set of all strings in A^*. The transition function is defined by concatenation, i.e. for a state $\alpha \in A^*$ and an action $a \in A$, $\mathtt{step}(\alpha, a) = \alpha a$. The observation functions are defined using the intransitive purge function associated to the above policy: $\mathtt{obs}_u(\alpha) = [\mathtt{ipurge}(\alpha, u)]$. (Here we put brackets around the sequence of actions when it is interpreted as an observation, to distinguish such occurrences from the actions themselves as they occur in a view.)

It is plain that M is IP-secure. For, if $\mathtt{ipurge}(\alpha, u) = \mathtt{ipurge}(\alpha', u)$ then $\mathtt{obs}_u(s_0 \cdot \alpha) = [\mathtt{ipurge}(\alpha, u)] = [\mathtt{ipurge}(\alpha', u)] = \mathtt{obs}_u(s_0 \cdot \alpha')$. We show that it does not satisfy condition (1).

Consider the sequences of actions $\alpha_1 = h_1h_2d_1d_2$ and $\alpha_2 = h_2h_1d_1d_2$. Note that these differ in the order of the events h_1, h_2. Let the atomic proposition p be interpreted by π as asserting that there is an occurrence of h_1 before an occurrence of h_2. That is, $\pi(p) = \{\alpha h_1 \beta h_2 \gamma \mid \alpha, \beta, \gamma \in A^*\}$.

Then we have $\mathtt{obs}_L(\alpha_1) = [\mathtt{ipurge}(\alpha_1, L)] = [h_1h_2d_1d_2]$. Hence, for any sequence α' with $\alpha_1 \equiv_u \alpha'$, we have $\mathtt{ipurge}_u(\alpha') = h_1h_2d_1d_2$, so $\alpha' \in \pi(p)$. Thus $M, \pi, \alpha_1 \models \mathtt{K}_L p$, i.e., in α_1 agent L knows the ordering of the events h_1, h_2. We demonstrate that α_2 is a witness showing that it is not the case that $M, \pi, \alpha_1 \models \mathtt{D}_{\{D_1,D_2\}} p$, i.e., we have $\alpha_1 \equiv_{\{D_1,D_2\}} \alpha_2$ and $\alpha_2 \notin \pi(p)$. The latter is trivial. For the former, note

$$\begin{aligned}
&\mathtt{view}_{D_1}(\alpha_1)\\
&\quad = \mathtt{obs}_{D_1}(\epsilon) \circ \mathtt{obs}_{D_1}(h_1) \circ \mathtt{obs}_{D_1}(h_1h_2) \circ d_1 \circ \mathtt{obs}_{D_1}(h_1h_2d_1) \circ \mathtt{obs}_{D_1}(h_1h_2d_1d_2)\\
&\quad = [\epsilon] \circ [h_1] \circ [h_1] \circ d_1 \circ [h_1d_1] \circ [h_1d_1]\\
&\quad = [\epsilon] \circ [\epsilon] \circ [h_1] \circ d_1 \circ [h_1d_1] \circ [h_1d_1]\\
&\quad = \mathtt{obs}_{D_1}(\epsilon) \circ \mathtt{obs}_{D_1}(h_2) \circ \mathtt{obs}_{D_1}(h_2h_1) \circ d_1 \circ \mathtt{obs}_{D_1}(h_2h_1d_1) \circ \mathtt{obs}_{D_1}(h_2h_1d_1d_2)\\
&\quad = \mathtt{view}_{D_1}(\alpha_2)
\end{aligned}$$

i.e., $\alpha_1 \equiv_{D_1} \alpha_2$. By symmetry, we also have $\alpha_1 \equiv_{D_2} \alpha_2$, hence $\alpha_1 \equiv_{\{D_1,D_2\}} \alpha_2$. This means that D_1 and D_2 do not have distributed knowledge of the ordering of the events h_1, h_2, even with respect to the asynchronous perfect recall intepretation of knowledge, in which they reason based on everything that they learn in the run.

Thus, L has acquired information that cannot have come from the two sources D_1 and D_2 that are supposed to be, according to the policy, its only sources of information. $\square$

3 Alternative Definitions

As a response to Example 1, we consider several alternative definitions of security for intransitive policies.

To begin, let us consider why it was felt to be necessary to modify the definition of P-security for the intransitive case. For this, note that the system of Example 1 is not P-secure. For example, if we take $\alpha = h_1 d_1$ and $\alpha' = d_1$ then $\texttt{purge}_L(\alpha) = d_1 = \texttt{purge}_L(\alpha')$ but $\texttt{obs}_L(s_0 \cdot \alpha) = [\alpha] \neq [\alpha'] = \texttt{obs}_L(s_0 \cdot \alpha')$. However, this particular instance does not seem like it should be a counterexample to the security of the system. Intuitively, the fact that L observations differ on $s_0 \cdot \alpha$ and $s_0 \cdot \alpha'$ is justifiable, on the grounds that the action d_1 "downgrades" to L the fact that action h_1 has been performed. Thus, whereas IP-security is too weak, P-security seems to be too strong, since it does not permit an agent to forward information that it has acquired.

We are lead to propose several other definitions of security. Each is based on a concrete model of the maximal amount of information that an agent may have after some sequence of actions has been performed, and states that an agent's observation may not give it more than this maximal amount of information. The definitions differ in the modelling of the maximal information, and take the view that an agent increases its information either by performing an action or by receiving information transmitted by another agent.

In the first model of the maximal information, what is transmitted when an agent performs an action is information about the actions performed by other agents. The following definition expresses this in a weaker way than the ipurge function.

Given sets X and A, let the set $\mathcal{T}(X, A)$ be the smallest set containing X and such that if $x, y \in \mathcal{T}$ and $z \in A$ then $(x, y, z) \in \mathcal{T}(X, A)$. Intuitively, the elements of $\mathcal{T}(X, A)$ are are binary trees with leaves labelled from X and interior nodes labelled from A.

Given a policy $\rightarrowtail$, define, for each agent $u \in D$, the function $\texttt{ta}_u : A^* \rightarrow \mathcal{T}(\{\epsilon\}, A)$ inductively by $\texttt{ta}_u(\epsilon) = \epsilon$, and, for $\alpha \in A^*$ and $a \in A$,

$$\texttt{ta}_u(\alpha a) = \begin{cases} \texttt{ta}_u(\alpha) & \text{when } \texttt{dom}(a) \not\rightarrowtail u, \\ (\texttt{ta}_u(\alpha), \texttt{ta}_{\texttt{dom}(a)}(\alpha), a) & \text{otherwise.} \end{cases}$$

Intuitively, $\texttt{ta}_u(\alpha)$ captures the maximal information that agent u may, consistently with the policy $\rightarrowtail$, have about the past actions of other agents. (The nomenclature is intended to be suggestive of *transmission* of information about *actions*.) Initially, an agent has no information about what actions have been performed. The recursive clause describes how the maximal information $\texttt{ta}_u(\alpha)$ permitted to u after the performance of α changes when the next action a is performed. If a may not interfere with u, then there is no change, otherwise, u's maximal permitted information is increased by adding the maximal information permitted to $\texttt{dom}(a)$ at the time a is performed (represented by $\texttt{ta}_{\texttt{dom}(a)}(\alpha)$), as well the fact that a has been performed. Thus, this definition captures the intuition that an agent may only transmit information that it is permitted to have, and then only to agents with which it is permitted to interfere.

Definition 3. *A system M is TA-secure with respect to a policy $\rightarrowtail$ if for all agents u and all $\alpha, \alpha' \in A^*$ such that $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha')$, we have $\mathtt{obs}_u(s_0 \cdot \alpha) = \mathtt{obs}_u(s_0 \cdot \alpha')$.*

Intuitively, this says that each agent's observations provide the agent with no more information than the maximal amount that may have been transmitted to it, as expressed by the functions $\mathtt{ta}$.

Example 2. Note that the system of Example 1 is not TA-secure. For,

$$\begin{aligned}
\mathtt{ta}_L(h_1h_2d_1d_2) &= (\mathtt{ta}_L(h_1h_2d_1), \mathtt{ta}_{D_2}(h_1h_2d_1), d_2) \\
&= ((\mathtt{ta}_L(h_1h_2), \mathtt{ta}_{D_1}(h_1h_2), d_1), \mathtt{ta}_{D_2}(h_1h_2), d_2) \\
&= ((\mathtt{ta}_L(h_1), \mathtt{ta}_{D_1}(h_1), d_1), (\mathtt{ta}_{D_2}(h_1), \mathtt{ta}_{H_2}(h_1), h_2), d_2) \\
&= ((\epsilon, (\epsilon, \epsilon, h_1), d_1), (\epsilon, \epsilon, h_2), d_2)
\end{aligned}$$

and

$$\begin{aligned}
\mathtt{ta}_L(h_2h_1d_1d_2) &= (\mathtt{ta}_L(h_2h_1d_1), \mathtt{ta}_{D_2}(h_2h_1d_1), d_2) \\
&= ((\mathtt{ta}_L(h_2h_1), \mathtt{ta}_{D_1}(h_2h_1), d_1), \mathtt{ta}_{D_2}(h_2h_1), d_2) \\
&= ((\mathtt{ta}_L(h_1), (\mathtt{ta}_{D_1}(h_2), \mathtt{ta}_{H_1}(h_2), h_1), d_1), \mathtt{ta}_{D_2}(h_2), d_2) \\
&= ((\epsilon, (\epsilon, \epsilon, h_1), d_1), (\epsilon, \epsilon, h_2), d_2).
\end{aligned}$$

So $\mathtt{ta}_L(h_1h_2d_1d_2) = \mathtt{ta}_L(h_2h_1d_1d_2)$, but $\mathtt{obs}_L(h_1h_2d_1d_2) = [h_1h_2d_1d_2] \neq [h_2h_1d_1d_2] = \mathtt{obs}_L(h_2h_1d_1d_2)$. This illustrates that TA-security is in accordance with our intuitions about Example 1. □

The definition of TA-security has one aspect that might plausibly be questioned: it classifies as secure situations in which an agent transmits information to another that it has not actually observed.

Example 3. Consider a downgrading system with policy $H \rightarrowtail D \rightarrowtail L$, actions $A = \{h, d, l\}$ of domains H, D, L, respectively, states A^* with $s_0 = \epsilon$ and transitions $\mathtt{step}(\alpha, a) = \alpha a$. Let the observation functions be given by $\mathtt{obs}_L(\alpha) = \mathtt{ta}_L(\alpha)$ and $\mathtt{obs}_u(\alpha) = \bot$ for all $\alpha \in A^*$ and $u \in \{H, D\}$. Let $\alpha, \alpha' \in \{h\}^*$. Then we have $\mathtt{ta}_D(\alpha) = \mathtt{ta}_D(\alpha')$ iff $\alpha \upharpoonright \{H, D\} = \alpha' \upharpoonright \{H, D\}$. Thus, from $\mathtt{obs}_L(\alpha d) = (\mathtt{ta}_L(\alpha), \mathtt{ta}_D(\alpha), d)$, it is possible for L to deduce the exact sequence of H actions performed in α. On the other hand, since always $\mathtt{obs}_D(\alpha) = \bot$, agent D itself has no information about this sequence. Thus, in this system, D can be viewed as causing information to be transmitted to L that it does not itself have. □

Whether one considers this example to illustrate a violation of security depends on one's attitude to forwarding of unobserved information. IP-security considers this acceptable, as does TA-security. However, it is possible to construct a definition that would consider this as insecure, by changing the definition of the function $\mathtt{ta}$.

Given a policy $\rightarrowtail$, for each domain $u \in D$, define the function $\mathtt{to}_u : A^* \to \mathcal{T}((A \cup O)^*, A)$ by $\mathtt{to}_u(\epsilon) = \mathtt{obs}_u(s_0)$ and

$$\mathtt{to}_u(\alpha a) = \begin{cases} \mathtt{to}_u(\alpha) & \text{when } \mathtt{dom}(a) \not\rightarrowtail u, \\ (\mathtt{to}_u(\alpha), \mathtt{view}_{\mathtt{dom}(a)}(\alpha), a) & \text{otherwise.} \end{cases}$$

Intuitively, this definition takes the model of the maximal information that an action a may transmit after the sequence α to be the fact that a has occurred, together with the information that $\mathtt{dom}(a)$ *actually* has, as represented by its view $\mathtt{view}_{\mathtt{dom}(a)}(\alpha)$. By contrast, TA-security uses in place of this the maximal information that $\mathtt{dom}(a)$ *may* have. (The nomenclature is intended to be suggestive of *transmission* of information about *observations.*) We may now base the definition of security on the function $\mathtt{to}$ rather than $\mathtt{ta}$.

Definition 4. *The system M is TO-secure with respect to $\rightarrowtail$ if for all domains $u \in D$ and all $\alpha, \alpha' \in A^*$ with $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha')$, we have $\mathtt{obs}_u(s_0 \cdot \alpha) = \mathtt{obs}_u(s_0 \cdot \alpha')$.*

We will also consider a slight variant of this definition. Given a policy $\rightarrowtail$, for each domain $u \in D$, define the function $\mathtt{ito}_u : A^* \to \mathcal{T}(O(A \cup O)^*, A)$ by $\mathtt{ito}_u(\epsilon) = \mathtt{obs}_u(s_0)$ and

$$\mathtt{ito}_u(\alpha a) = \begin{cases} \mathtt{ito}_u(\alpha) & \text{if } \mathtt{dom}(a) \not\rightarrowtail u, \\ (\mathtt{ito}_u(\alpha), \mathtt{view}_{\mathtt{dom}(a)}(\alpha), a) & \text{if } \mathtt{dom}(a) = u, \\ (\mathtt{ito}_u(\alpha), \mathtt{view}_{\mathtt{dom}(a)}(\alpha a), a) & \text{otherwise.} \end{cases}$$

This definition is just like that of $\mathtt{to}$, with the difference that the information that may be transmitted to u by an action a such that $\mathtt{dom}(a) \rightarrowtail u$ but $\mathtt{dom}(a) \neq u$, includes the observation $\mathtt{obs}_{\mathtt{dom}(a)}(s_0 \cdot \alpha a)$ obtained in domain $\mathtt{dom}(a)$ immediately after the occurrence of action a. Intuitively, the definition of security based on this notion will allow that the action a transmits not just the information observable to $\mathtt{dom}(a)$ at the time that it is invoked, but also the new information that it computes and makes observable in $\mathtt{dom}(a)$. This information is not included in the value $\mathtt{ito}_{\mathtt{dom}(a)}(\alpha a)$ itself, since the definition of security will state that the new observation may depend only on this value. The nomenclature in this case is intended to be suggestive of *immediate* transmission of information about observations.

The following definition follows the pattern of the others, but based is on the functions $\mathtt{ito}$.

Definition 5. *The system M is ITO-secure with respect to $\rightarrowtail$ if for all domains $u \in D$ and all $\alpha, \alpha' \in A^*$ with $\mathtt{ito}_u(\alpha) = \mathtt{ito}_u(\alpha')$, we have $\mathtt{obs}_u(s_0 \cdot \alpha) = \mathtt{obs}_u(s_0 \cdot \alpha')$.*

We now consider how all these definitions of security are related. We begin by noting that it is possible to give a flatter representation of the information in $\mathtt{to}_u(\alpha)$, that clarifies the relationship of this notion to P-security. Define the *possibly transmitted view* of domain u for a sequence of actions α to be the largest prefix $\mathtt{tview}_u(\alpha)$ of $\mathtt{view}_u(\alpha)$ than ends in an action a with $\mathtt{dom}(a) = u$. Then we have the following result, which intuitively says that u's observations depend only on (1) the parts of the views of other agents which are permitted to pass information to u, that they have actually acted to transmit, and (2) u's knowledge of the ordering of its own actions and the actions of these other agents.

Proposition 1. *M is TO-secure with respect to a policy $\rightarrowtail$ iff for all sequences $\alpha, \alpha' \in A^*$, and domains $u \in D$, if $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\alpha')$ and $\mathtt{tview}_v(\alpha) = \mathtt{tview}_v(\alpha')$ for all domains $v \neq u$ such that $v \rightarrowtail u$, then $\mathtt{obs}_u(s_0 \cdot \alpha) = \mathtt{obs}_u(s_0 \cdot \alpha')$.*

Proof. We show that $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha')$ iff $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\alpha')$ and $\mathtt{tview}_v(\alpha) = \mathtt{tview}_v(\alpha')$ for all domains $v \neq u$ such that $v \rightarrowtail u$.

For the proof from left to right, we proceed by induction on the combined length of α and α'. The base case is trivial.

1. Supposing the claim holds for strings of shorter combined length, consider strings αa and α' such that $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha')$ where $a \in A$ and $\mathtt{dom}(a) \not\rightarrowtail u$. Then $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha')$, so by induction, we have that $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\alpha')$ and $\mathtt{tview}_v(\alpha) = \mathtt{tview}_v(\alpha')$ for all domains $v \neq u$ such that $v \rightarrowtail u$. Since $\mathtt{dom}(a) \not\rightarrowtail u$, we have $\mathtt{purge}_u(\alpha a) = \mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\alpha')$. Similarly, we have that $\mathtt{dom}(a) \neq v$ for any v such that $v \rightarrowtail u$, so $\mathtt{tview}_v(\alpha a) = \mathtt{tview}_v(\alpha) = \mathtt{tview}_v(\alpha')$ for all domains $v \neq u$ such that $v \rightarrowtail u$, as required.
2. Alternately, suppose $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha')$ where $\mathtt{dom}(a) \rightarrowtail u$. Then α' cannot be ϵ. If the last action of α' does not interfere with u then we may apply the previous case. Hence, without loss of generality, $\alpha' = \beta b$ where $\mathtt{dom}(b) \rightarrowtail u$, and from $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\beta b)$ we obtain $a = b$, $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\beta)$, and $\mathtt{view}_{\mathtt{dom}(a)}(\alpha) = \mathtt{view}_{\mathtt{dom}(a)}(\beta)$.
   From $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\beta)$, we have by the induction hypothesis that $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\alpha')$ and $\mathtt{tview}_v(\alpha) = \mathtt{tview}_v(\alpha')$ for all domains $v \neq u$ such that $v \rightarrowtail u$. It follows that $\mathtt{purge}_u(\alpha a) = \mathtt{purge}_u(\alpha) \cdot a = \mathtt{purge}_u(\beta) \cdot a = \mathtt{purge}_u(\beta a)$. Further, it follows that $\mathtt{tview}_v(\alpha a) = \mathtt{tview}_v(\beta a)$ for $v \neq u$ such that $v \rightarrowtail u$. The proof of this is in two cases: (1) if $v = \mathtt{dom}(a)$, then $\mathtt{tview}_v(\alpha a) = \mathtt{view}_v(\alpha) \cdot a = \mathtt{view}_v(\beta) \cdot a = \mathtt{tview}_v(\beta a)$; (2) if $v \neq \mathtt{dom}(a)$ then $\mathtt{tview}_v(\alpha a) = \mathtt{tview}_v(\alpha) = \mathtt{tview}_v(\beta) = \mathtt{tview}_v(\beta a)$.

Conversely, for the implication from right to left, we again proceed by induction on the combined length of α and α'. The base case of $\alpha = \alpha' = \epsilon$ is trivial.

1. Consider the case where the RHS holds for αa and α', where $\mathtt{dom}(a) \not\rightarrowtail u$, and the implication from right to left holds for α, α'. Then from $\mathtt{purge}_u(\alpha a) = \mathtt{purge}_u(\alpha')$ we obtain that $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\alpha')$. Similarly, for $v \neq u$, $v \rightarrowtail u$, we have $\mathtt{tview}_v(\alpha a) = \mathtt{tview}_v(\alpha')$, so, since we cannot have $v = \mathtt{dom}(a)$ in the present case, we obtain that $\mathtt{tview}_v(\alpha) = \mathtt{tview}_v(\alpha a) = \mathtt{tview}_v(\alpha')$. By the inductive hypothesis, it follows that $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha')$, hence $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha')$.
2. Consider the case where the RHS holds for αa and α', where $\mathtt{dom}(a) \rightarrowtail u$, and the implication from right to left holds for α, α'. Since $\mathtt{purge}_u(\alpha') = \mathtt{purge}_u(\alpha a) = \mathtt{purge}_u(\alpha)\, a$, the sequence α' cannot be ϵ. We may assume without loss of generality that $\alpha' = \beta b$ where $\mathtt{dom}(b) \rightarrowtail u$, else we may apply the previous case. Thus, from $\mathtt{purge}_u(\alpha a) = \mathtt{purge}_u(\beta b)$ it follows that $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\beta)$ and $a = b$. We claim that moreover (1) $\mathtt{to}_u(\alpha) =$

$\mathtt{to}_u(\beta)$ and (2) $\mathtt{view}_{\mathtt{dom}(a)}(\alpha) = \mathtt{view}_{\mathtt{dom}(a)}(\beta)$, from which it follows that $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\beta b)$, which is the conclusion required.
We prove (2) first. Since $\mathtt{dom}(a) \rightarrowtail u$, $\mathtt{dom}(a)$ is one of the domains v for which we have $\mathtt{tview}_v(\alpha a) = \mathtt{tview}_v(\beta a)$. It follows that $\mathtt{view}_{\mathtt{dom}(a)}(\alpha) = \mathtt{view}_{\mathtt{dom}(a)}(\beta)$, which is (2). Moreover, it also follows from (2) that $\mathtt{tview}_{\mathtt{dom}(a)}(\alpha) = \mathtt{tview}_{\mathtt{dom}(a)}\beta)$. For all other domains $v \neq \mathtt{dom}(a)$ such that $v \rightarrowtail u$, we have $\mathtt{tview}_v(\alpha) = \mathtt{tview}_v(\alpha a) = \mathtt{tview}_v(\beta a) = \mathtt{tview}_v(\beta)$, so in fact the second part of the antecedant of the induction hypothesis is satisfied. Since we already have the first part, i.e., $\mathtt{purge}_u(\alpha) = \mathtt{purge}_u(\beta)$, we obtain (1).

□

We note the following property of these definitions:

Proposition 2. *Let* $\alpha, \alpha' \in A^*$ *and* $u \in D$.

1. *If* M *is TO-secure and* $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha')$ *then* $\mathtt{view}_u(\alpha) = \mathtt{view}_u(\alpha')$.
2. *If* M *is ITO-secure and* $\mathtt{ito}_u(\alpha) = \mathtt{ito}_u(\alpha')$ *then* $\mathtt{view}_u(\alpha) = \mathtt{view}_u(\alpha')$.
3. *If* M *is TA-secure and* $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha')$ *then* $\mathtt{view}_u(\alpha) = \mathtt{view}_u(\alpha')$.

Proof. By induction on $|\alpha|+|\alpha'|$. We give the proof for (1), the proofs for (2) and (3) follow a similar structure. The base case of $\alpha = \alpha' = \epsilon$ is trivial. Consider sequences of actions αa and α', where $a \in A$, such that $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha')$.

If $\mathtt{dom}(a) \not\rightarrowtail u$, then we have $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha')$. By the induction hypothesis we get that $\mathtt{view}_u(\alpha) = \mathtt{view}_u(\alpha')$. Since $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha)$, we get from TO-security that $\mathtt{obs}_u(s_0 \cdot \alpha a) = \mathtt{obs}_u(s_0 \cdot \alpha)$, which implies that $\mathtt{view}_u(\alpha a) = \mathtt{view}_u(\alpha) \circ \mathtt{obs}_u(s_0 \cdot \alpha a) = \mathtt{view}_u(\alpha) \circ \mathtt{obs}_u(s_0 \cdot \alpha) = \mathtt{view}_u(\alpha)$. (Note that $\mathtt{dom}(a) \not\rightarrowtail u$ implies $\mathtt{dom}(a) \neq u$.) It follows that $\mathtt{view}_u(\alpha a) = \mathtt{view}_u(\alpha')$.

If $\mathtt{dom}(a) \not\rightarrowtail u$, then $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha')$ implies that $\alpha' \neq \epsilon$. Let b be the final action in α', so that $\alpha' = \beta b$. If $\mathtt{dom}(b) \not\rightarrowtail u$, then we may apply the previous case with the roles of αa and βb swapped, so we may assume that $\mathtt{dom}(b) \rightarrowtail u$. It then follows from $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\beta b)$ that $a = b$ and $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\beta)$. By the inductive hypothesis we get that $\mathtt{view}_u(\alpha) = \mathtt{view}_u(\beta)$. From TO-security and $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\beta a)$ we get that $\mathtt{obs}_u(s_0 \cdot \alpha a) = \mathtt{obs}_u(s_0 \cdot \beta a)$. It now follows in both the case that $\mathtt{dom}(a) = u$ and the case that $\mathtt{dom}(a) \neq u$ that $\mathtt{view}_u(\alpha a) = \mathtt{view}_u(\beta a)$, as required. □

The following result describes how these definitions are related. Like IP-security, the notions P-security, TO-security, ITO-security and TA-security are generalizations of the classical notion of noninterference in the transitive case.

Theorem 1.

1. *If* M *is P-secure with respect to* $\rightarrowtail$ *then* M *is TO-secure with respect to* $\rightarrowtail$.
2. *If* M *is TO-secure with respect to* $\rightarrowtail$ *then* M *is ITO-secure with respect to* $\rightarrowtail$.
3. *If* M *is ITO-secure with respect to* $\rightarrowtail$ *then* M *is TA-secure with respect to* $\rightarrowtail$.
4. *If* M *is TA-secure with respect to* $\rightarrowtail$ *then* M *is IP-secure with respect to* $\rightarrowtail$.

5. *If $\rightarrowtail$ is transitive then P-security, TO-security, ITO-security, TA-security and IP-security (all with respect to $\rightarrowtail$) are equivalent.*

Proof. Part (1) is immediate from Proposition 1. Part (5) follows from parts (1)-(4), using the fact that P-security and IP-security are equivalent with respect to transitive policies (Rushby [Rus92] Theorem 9).

For part (2), we claim that if $\mathtt{ito}_u(\alpha) = \mathtt{ito}_u(\alpha')$ then $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha')$. Part (2) then follows trivially. To see that the claim holds, define the partial functions $F_u : \mathcal{T}((A \cup O)^*, A) \to \mathcal{T}((A \cup O)^*, A)$, for $u \in D$, defined inductively by $F_u(\epsilon) = \epsilon$ and $F_u(X, \sigma a o, a) = (F_u(X), \sigma, a)$, where $o \in O$ and $\mathtt{dom}(a) \neq u$, and $F_u(X, \sigma, a) = (F_u(X), \sigma, a)$ when $\mathtt{dom}(a) = u$. Then it is easily shown that $F_u(\mathtt{ito}_u(\alpha)) = \mathtt{to}_u(\alpha)$ for all $\alpha \in A^*$, from which the claim is immediate.

We now prove part (3). Assume that M is ITO-secure with respect to $\rightarrowtail$. We claim that for all $u \in D$ and $\alpha, \alpha' \in A^*$, if $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha')$ then $\mathtt{ito}_u(\alpha) = \mathtt{ito}_u(\alpha')$. The result is then immediate from the definition of TO-security. The proof of the claim is by induction on $|\alpha| + |\alpha'|$. The base case of $\alpha = \alpha' = \epsilon$ is trivial. Supposing that the claim holds for strings of shorter combined length, suppose $\mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha')$, where $\alpha, \alpha' \in A^*$ and $a \in A$. We consider two cases:

Case 1: $\mathtt{dom}(a) \not\rightarrowtail u$. Then $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha')$, so by the inductive hypothesis we have $\mathtt{ito}_u(\alpha) = \mathtt{ito}_u(\alpha')$. Since $\mathtt{ito}_u(\alpha a) = \mathtt{ito}_u(\alpha)$ in this case, it is immediate that $\mathtt{ito}_u(\alpha a) = \mathtt{ito}_u(\alpha')$.

Case 2: $\mathtt{dom}(a) \rightarrowtail u$. We may assume without loss of generality that the last action in α' also interferes with u, else we may apply the previous case. So let $\alpha' = \beta b$ with $\mathtt{dom}(b) \rightarrowtail u$. Then $\mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\beta b)$, from which we get that $a = b$ and $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\beta)$ and $\mathtt{ta}_{\mathtt{dom}(a)}(\alpha) = \mathtt{ta}_{\mathtt{dom}(a)}(\beta)$. By induction, we have that $\mathtt{ito}_u(\alpha) = \mathtt{ito}_u(\beta)$ and $\mathtt{ito}_{\mathtt{dom}(a)}(\alpha) = \mathtt{ito}_{\mathtt{dom}(a)}(\beta)$. From the latter, we obtain by ITO-security and Proposition 2 that $\mathtt{view}_{\mathtt{dom}(a)}(\alpha) = \mathtt{view}_{\mathtt{dom}(a)}(\beta)$. Together with $\mathtt{ito}_{\mathtt{dom}(a)}(\alpha) = \mathtt{ito}_{\mathtt{dom}(a)}(\beta)$ this yields that $\mathtt{ito}_{\mathtt{dom}(a)}(\alpha a) = \mathtt{ito}_{\mathtt{dom}(a)}(\beta a)$, so by ITO-security, we have $\mathtt{obs}_{\mathtt{dom}(a)}(s_0 \cdot \alpha a) = \mathtt{obs}_{\mathtt{dom}(a)}(s_0 \cdot \beta a)$. Thus, we also have the stronger statement $\mathtt{view}_{\mathtt{dom}(a)}(\alpha a) = \mathtt{view}_{\mathtt{dom}(a)}(\beta a)$. It now follows, in both the case that $\mathtt{dom}(a) = u$ and $\mathtt{dom}(a) \neq u$, that $\mathtt{ito}_u(\alpha a) = \mathtt{ito}_u(\beta b)$.

To show part (4), we claim that if $u \in X \subseteq D$ then $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\mathtt{ipurge}_X(\alpha))$. In particular, $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\mathtt{ipurge}_u(\alpha))$. Note that this straightforwardly implies that if $\mathtt{ipurge}_u(\alpha) = \mathtt{ipurge}_u(\alpha')$ then $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha')$, and so if M is TA-secure with respect to $\rightarrowtail$ then M is IP-secure with respect to $\rightarrowtail$. To prove the claim we proceed by induction. The case of $\alpha = \epsilon$ is trivial. Assuming the claim holds for α, consider αa where $a \in A$. We consider two cases, depending on whether $\mathtt{dom}(a) \rightarrowtail u$.

If $\mathtt{dom}(a) \not\rightarrowtail u$, then $\mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha)$. We consider two further subscases. Write $v \rightarrowtail X$ if there exists $w \in X$ such that $v \rightarrowtail w$.

Case 1: $\mathtt{dom}(a) \not\rightarrowtail X$. Then $\mathtt{ipurge}_X(\alpha a) = \mathtt{ipurge}_X(\alpha)$. Hence

$$\begin{aligned} \mathtt{ta}_u(\mathtt{ipurge}_X(\alpha a)) &= \mathtt{ta}_u(\mathtt{ipurge}_X(\alpha)) \\ &= \mathtt{ta}_u(\alpha) \qquad \text{(by induction)} \\ &= \mathtt{ta}_u(\alpha a). \end{aligned}$$

Case 2: $\texttt{dom}(a) \rightarrowtail X$. Then $\texttt{ipurge}_X(\alpha a) = \texttt{ipurge}_{X\cup\{\texttt{dom}(a)\}}(\alpha)\cdot a$. Hence, from the induction hypothesis and the definitions,

$$\begin{aligned}
\texttt{ta}_u(\texttt{ipurge}_X(\alpha a)) &= \texttt{ta}_u(\texttt{ipurge}_{X\cup\{\texttt{dom}(a)\}}(\alpha)\cdot a)\\
&= \texttt{ta}_u(\texttt{ipurge}_{X\cup\{\texttt{dom}(a)\}}(\alpha))\\
&= \texttt{ta}_u(\alpha) && \text{(by induction)}\\
&= \texttt{ta}_u(\alpha a).
\end{aligned}$$

If $\texttt{dom}(a) \rightarrowtail u$, then $\texttt{ipurge}_X(\alpha a) = \texttt{ipurge}_{X\cup\{\texttt{dom}(a)\}}(\alpha)\cdot a$. Thus

$$\begin{aligned}
\texttt{ta}_u(\texttt{ipurge}_u(\alpha a)) &= \texttt{ta}_u(\texttt{ipurge}_{X\cup\{\texttt{dom}(a)\}}(\alpha)\cdot a)\\
&= (\texttt{ta}_u(\texttt{ipurge}_{X\cup\{\texttt{dom}(a)\}}(\alpha)), \texttt{ta}_{\texttt{dom}(a)}(\texttt{ipurge}_{X\cup\{\texttt{dom}(a)\}}(\alpha)), a)\\
&= (\texttt{ta}_u(\alpha), \texttt{ta}_{\texttt{dom}(a)}(\alpha), a) \qquad \text{(by induction)}\\
&= \texttt{ta}_u(\alpha a).
\end{aligned}$$

This completes the proof of the claim. □

Roscoe and Goldsmith [RG99] have also proposed alternate definitions of security based on intransitive noninterference, working in the context of the process algebra CSP. The question of how exactly our defintions relate to RG's definitions requires a treatment of mappings between state machine models and CSP, for which there are a number of plausible candidates. We deal with this topic in another paper [Mey07a], where we show that one transformation yields that RG's definition is in fact P-security, but on another transformation, another of RG's definitions that generalises the first turns out to be equivalent to ITO-security.

We will focus in what follows on the properties TA-security and TO-security, but have included ITO-security in the discussion above to show how RG's definitions of intransitive noninterference fit into the spectrum of possibilities.

4 Unwinding Relations

In this section we relate our alternative definitions of security for intransitive policies to "unwinding conditions" that have been discussed in the literature as a way to prove noninterference [GM84]. We show that Rushby's proposed unwinding conditions for intransitive noninterference are most closely related to the notion of TA-security (where they provide a sound and complete proof method), although they are also sufficient for TO-security in a special case. We also show the somewhat suprising fact that Rushby's unwinding conditions are not preserved under bisimulation.

We begin by recalling Rushby's results on unwinding for intransitive nonintereference. Suppose we have for each domain u an equivalence relation $\sim_u$ on the states of M. Rushby discusses the following "unwinding" conditions on such equivalence relations.

OC: If $s \sim_u t$ then $\texttt{obs}_u(s) = \texttt{obs}_u(t)$. (Output Consistency)

SC: If $s \sim_u t$ then $s \cdot a \sim_u t \cdot a$. (Step Consistency)
LR: If $\mathtt{dom}(a) \not\rightarrowtail u$ then $s \sim_u s \cdot a$. (Left Respect)

If these conditions are satisfied and $\rightarrowtail$ is a transitive policy, then M is P-secure [GM84]. Conversely, consider the particular equivalence relations $\approx_u$ on states, defined by $s \approx_u t$ if for all strings α in A^* we have $\mathtt{obs}_u(s \cdot \alpha) = \mathtt{obs}_u(t \cdot \alpha)$. Rushby uses these equivalence relations to show completeness of the unwinding conditions for transitive noninterference:

Proposition 3. *([Rus92] Theorem 6) Suppose M is P-secure with respect to the transitive policy $\rightarrowtail$. Then the relations $\approx_u$ satisfy OC, SC and LR.*

For intransitive noninterference he introduces the following condition:

WSC: If $s \sim_u t$ and $s \sim_{dom(a)} t$ then $s \cdot a \sim_u t \cdot a$. (Weak Step Consistency)

Define a *weak unwinding* on a system M with respect to a policy $\rightarrowtail$ to be a family of relations $\sim_u$, for $u \in D$, satisfying OC,WSC and LR. It will be convenient to have the following alternate characterization of this notion. Given a system M and a policy $\rightarrowtail$, let $\{\approx_u^{\mathrm{uw}}\}_{u\in D}$ be the smallest family of equivalence relations (under the pointwise containment order) satisfying WSC and LR.

Proposition 4. *There exists a weak unwinding for M with respect to $\rightarrowtail$ iff the relations $\approx_u^{\mathrm{uw}}$ satisfy OC.*

Proof. The implication from right to left is trivial. For the implication from left to right, suppose that $\{\sim_u\}_{u\in D}$ is a weak unwinding for M with respect to $\rightarrowtail$. It is immediate from the definition of $\approx_u^{\mathrm{uw}}$ and fact that the property of being an equivalence relation satisfying WSC and LR is defined by Horn formulas that $\approx_u^{\mathrm{uw}} \subseteq \sim_u$. The fact that $\sim_u$ satisfies OC now implies that $\approx_u^{\mathrm{uw}}$ satisfies OC. $\square$

Rushby shows the following:

Proposition 5. *([Rus92], Theorem 7) Suppose that the relations $\{\sim_u\}_{u\in D}$ on a system M satisfy OC,WSC and LR. Then M is IP-secure for $\rightarrowtail$.*

However, he does not establish completeness of these unwinding conditions for IP-security. The following result yields an explanation of this fact.

Theorem 2. *Suppose that there exists a weak unwinding for M with respect to $\rightarrowtail$. Then M is TA-secure with respect to $\rightarrowtail$.*

Proof. Let the weak unwinding be $\{\sim_u\}_{u\in D}$. We show that for $u \in D$ and $\alpha, \alpha' \in A^*$, if $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha')$ then $s_0 \cdot \alpha \sim_u s_0 \cdot \alpha'$. By OC, it also follows that $\mathtt{obs}_u(s_0 \cdot \alpha) = \mathtt{obs}_u(s_0 \cdot \alpha')$, which is what we need for TA-security. We proceed by induction on $|\alpha| + |\alpha'|$. The base case of $\alpha = \alpha' = \epsilon$ is trivial. Supposing that the result holds for sequences of shorter combined length, consider sequences αa and α', where $a \in A$ and $\mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha')$.

If $\mathtt{dom}(a) \not\rightarrowtail u$, then $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha')$. Hence, by induction, $s_0 \cdot \alpha \sim_u s_0 \cdot \alpha'$. Also, by LR, we have $s_0 \cdot \alpha a \sim_u s_0 \cdot \alpha$, Thus $s_0 \cdot \alpha a \sim_u s_0 \cdot \alpha'$ by transitivity of $\sim_u$.

If $\mathtt{dom}(a) \rightarrowtail u$, then $\mathtt{ta}_u(\alpha a) = (\mathtt{ta}_u(\alpha), \mathtt{ta}_{\mathtt{dom}(a)}(\alpha), a)$, which implies that the action a also occurs in α' as the last action in a domain interfering with u. If there are any subsequent noninterfering actions, we may switch the role of αa and α' and apply the previous case. Hence, we may assume $\alpha' = \beta a$ for some sequence of actions β, so $\mathtt{ta}_u(\alpha') = (\mathtt{ta}_u(\beta), \mathtt{ta}_{\mathtt{dom}(a)}(\beta), a)$. It follows from the equality $\mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha')$ that $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\beta)$ and $\mathtt{ta}_{\mathtt{dom}(a)}(\alpha) = \mathtt{ta}_{\mathtt{dom}(a)}(\beta)$. By the inductive hypothesis, we obtain $s_0 \cdot \alpha \sim_u s_0 \cdot \beta$ and $s_0 \cdot \alpha \sim_{\mathtt{dom}(a)} s_0 \cdot \beta$. It follows from this by WSC that $s_0 \cdot \alpha a \sim_u s_0 \cdot \beta a$. $\square$

Since, by Example 2, TA-security is stronger than IP-security, this result implies that the existence of equivalence relations $\sim_u$ satisfying conditions OC, WSC and LR is *not* a necessary condition for IP-security, since if this were the case, then every IP-secure system would be TA-secure.

This raises the question of whether the existence of weak unwindings is equivalent to TA-security instead. We now show that this question can be answered in the positive, provided it is formulated appropriately. The existence of weak unwindings turns out to have a somewhat surprising dependency on the structure of the system.

Given a system $M = \langle S, s_0, \mathtt{step}, \mathtt{obs}, \mathtt{dom}\rangle$ with actions A, define the "unfolded" system $\mathtt{uf}(M) = \langle S', s_0', \mathtt{step}', \mathtt{obs}', \mathtt{dom}\rangle$ with actions A having the same domains as in M, by $S' = A^*$, $s_0' = \epsilon$, $\mathtt{step}'(\alpha, a) = \alpha a$, and $\mathtt{obs}'_u(\alpha) = \mathtt{obs}_u(s_0 \cdot \alpha)$, where $s_0 \cdot \alpha$ is computed in M. Intuitively, this construction unfolds the graph of M into an infinite tree. Then we have the following.

Theorem 3. *M is TA-secure with respect to $\rightarrowtail$ iff there exists a weak unwinding on $\mathtt{uf}(M)$ with respect to $\rightarrowtail$.*

Proof. Define the equivalence relations $\sim_u^{\mathtt{ta}}$ on $\mathtt{uf}(M)$ by $\alpha \sim_u^{\mathtt{ta}} \alpha'$ iff $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha')$. We first note that for the relations $\approx_u^{\mathrm{uw}}$ on $\mathtt{uf}(M)$, we have $\alpha \approx_u^{\mathrm{uw}} \alpha'$ iff $\alpha \sim_u^{\mathtt{ta}} \alpha'$. For, the relations $\sim_u^{\mathtt{ta}}$ are equivalence relations and satisfy WSC and LR by definition of $\mathtt{ta}_u$. Thus, we have $\approx_u^{\mathrm{uw}} \subseteq \sim_u^{\mathtt{ta}}$ by definition of $\approx_u^{\mathrm{uw}}$. Conversely, we show that $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha')$ implies $\alpha \approx_u^{\mathrm{uw}} \alpha'$, by induction on $|\alpha| + |\alpha'|$. The case of $\alpha = \alpha' = \epsilon$ is clear. Suppose $\mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha')$. If $\mathtt{dom}(a) \not\rightarrowtail u$, we have $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\alpha a) = \mathtt{ta}_u(\alpha')$, so by the inductive hypothesis, we have $\alpha \approx_u^{\mathrm{uw}} \alpha'$. Since $\approx_u^{\mathrm{uw}}$ satisfies LR, we obtain $\alpha a \approx_u^{\mathrm{uw}} \alpha$ and it follows that $\alpha a \approx_u^{\mathrm{uw}} \alpha'$. For the case $\mathtt{dom}(a) \rightarrowtail u$, where $\mathtt{ta}_u(\alpha a) = (\mathtt{ta}_u(\alpha), \mathtt{ta}_{\mathtt{dom}(a)}(\alpha), a)$, we may assume without loss of generality that the final action in α' may interfere with u, and derive that $\alpha' = \beta a$ where $\mathtt{ta}_u(\alpha) = \mathtt{ta}_u(\beta)$ and $\mathtt{ta}_{\mathtt{dom}(a)}(\alpha) = \mathtt{ta}_{\mathtt{dom}(a)}(\beta)$. It follows by the inductive hypothesis that $\alpha \approx_u^{\mathrm{uw}} \beta$ and $\alpha \approx_{\mathtt{dom}(a)}^{\mathrm{uw}} \beta$, hence by the fact that $\approx_u^{\mathrm{uw}}$ satisfies WSC that $\alpha a \approx_u^{\mathrm{uw}} \beta a$, as required.

Suppose M is TA-secure with respect to $\rightarrowtail$. Then WSC and LR for the relations $\sim_u^{\mathtt{ta}}$ are immediate from the definition of the functions $\mathtt{ta}_u$, and OC follows directly from TA-security. Hence the family $\sim_u^{\mathtt{ta}}$ is a weak unwinding on

$\mathtt{uf}(M)$. Conversely, suppose that there exists a weak unwinding $\sim_u$ on $\mathtt{uf}(M)$ with respect to $\rightarrowtail$. Then $\sim_u^{\mathtt{ta}} = \approx_u^{\mathrm{uw}} \subseteq \sim_u$ satisfies OC, hence M is TA-secure with respect to $\rightarrowtail$. □

It is reasonable to give a definition of security on M by reference to $\mathtt{uf}(M)$ since these systems are bisimilar under the obvious notion of bisimulation on the state-observed system model. Bisimilarity of two systems is usually taken to imply their equivalence on all properties of interest. One might therefore expect from Theorem 3 that TA-security implies the existence of a weak unwinding on the system M as well as on $\mathtt{uf}(M)$. It is the case that unwindings on M can be lifted to unwindings on $\mathtt{uf}(M)$.

Proposition 6. *If there exists a weak unwinding for $\rightarrowtail$ on M then there exists a weak unwinding for $\rightarrowtail$ on $\mathtt{uf}(M)$*

Proof. Suppose the relations $\sim_u$ are a weak unwinding for $\rightarrowtail$ on M. Define $\sim_u'$ on $\mathtt{uf}(M)$ by $\alpha \sim_u' \alpha'$ if $s_0 \cdot \alpha \sim_u s_0 \cdot \alpha'$ in M. It is easily checked that the relations $\sim_u'$ are a weak unwinding on $\mathtt{uf}(M)$. □

However, what we need, given Theorem 3, to deduce the existence of an unwinding on M from TA-security is the converse of this result. The following example shows that the converse does not hold. The reader may obtain some intuition for this example by noting that whereas weak unwinding seems to be sensitive to information about past actions, bisimulation cares only about the future. The essence of the example is that not enough past information is encoded in the states of the system M itself.

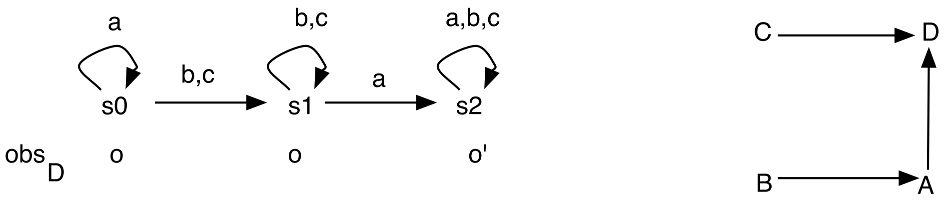

Fig. 1. An example showing TA-security does not imply existence of a weak unwinding.

Example 4. Consider the system and policy depicted in Figure 1. There are actions a, b, c of domains $\mathtt{A}, \mathtt{B}, \mathtt{C}$ respectively, and s_0 is the initial state. For all domains u other than $\mathtt{D}$, we assume that the observation $\mathtt{obs}_u$ is the same on all states. TA-security therefore depends only on the behaviour of the system with respect to domain $\mathtt{D}$, where there are two possible observations o, o' as indicated. We show that there does not exist a weak unwinding for $\rightarrowtail$ on M, but there does exist one on $\mathtt{uf}(M)$.

For the former, we consider the relation family $\approx_u^{\mathrm{uw}}$ on M. Note that since $\mathtt{B} \not\rightarrowtail \mathtt{D}$ and $s_0 \cdot b = s_1$ we have by LR that $s_0 \approx_{\mathtt{D}}^{\mathrm{uw}} s_1$. Similarly, since $\mathtt{C} \not\rightarrowtail \mathtt{A}$ we have $s_0 \approx_{\mathtt{A}}^{\mathrm{uw}} s_1$. Hence, by WSC, for the action a, we get $s_0 \approx_{\mathtt{D}}^{\mathrm{uw}} s_2$. Since $\mathtt{obs}_{\mathtt{D}}(s_0) = o$ and $\mathtt{obs}_{\mathtt{D}}(s_2) = o'$, we have that $\approx_{\mathtt{D}}^{\mathrm{uw}}$ does not satisfy OC. Since $\approx_u^{\mathrm{uw}}$ is the smallest family satisfying WSC and LR, there can exist no weak unwinding for $\rightarrowtail$ on M.

For the unwinding on $\mathtt{uf}(M)$, consider $\approx_u^{\mathrm{uw}} = \sim_u^{\mathtt{ta}}$. Since this family of equivalence relations satisfies WSC and LR, it suffices to consider the property OC, where we need consider only the domain $\mathtt{D}$, as already noted. Here, the only possible failure of OC is for states α, α' where $\mathtt{ta}_{\mathtt{D}}(\alpha) = \mathtt{ta}_{\mathtt{D}}(\alpha')$, $s_0 \cdot \alpha \in \{s_0, s_1\}$ and $s_0 \cdot \alpha' = s_2$. Now $s_0 \cdot \alpha' = s_2$ implies that α' contains either a b and a later a, or a c and a later a. View $\mathtt{ta}_{\mathtt{D}}(\alpha')$ as a tree with nodes of the form (x, y, e) representing a vertex labelled e with subtrees corresponding to x and y. Then this tree contains a path from a leaf to the root containing either b and later a, or c and later a. The same then applies to the identical tree for $\mathtt{ta}_{\mathtt{D}}(\alpha)$, which implies that α contains either a b and later a or a c and later a. But this means that $s_0 \cdot \alpha = s_2$, a contradiction. Hence the family $\approx_u^{\mathrm{uw}}$ satisfies OC. □

Since $\mathtt{uf}(M)$ and M are bisimilar, this example shows that bisimulation does not preserve existence of a weak unwinding. It is therefore necessary to either abandon the presumption that security properties are preserved under bisimulation, or adopt the stance that existence of a weak unwinding (on the system as presented) is not a sensible notion of security. We prefer the latter, but note that this does not hinder the utility of weak unwinding as a proof technique.

Further evidence of the utility of weak unwinding is the following result, which shows that it can also be used as a proof technique for TO-security. Define the relations $\approx_u^{\mathtt{obs}}$ on states of a system M by $s \approx_u^{\mathtt{obs}} t$ if $\mathtt{obs}_u(s) = \mathtt{obs}_u(t)$. Then we have the following sufficient condition for TO-security:

Proposition 7. *Suppose the relation family $\approx_u^{\mathtt{obs}}$ is a weak unwinding on M with respect to $\rightarrowtail$. Then M is TO-secure with respect to $\rightarrowtail$.*

Proof. We claim that $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha')$ implies $s_0 \cdot \alpha \approx_u^{\mathtt{obs}} s_0 \cdot \alpha'$. The result then follows immediately using OC. The proof of the claim is by induction on the combined length of the sequences α, α'. In case both are ϵ, the claim plainly holds. Suppose that it holds for sequences of shorter combined length, and consider the sequences αa and α', where $a \in A$. We consider two cases, depending on whether $\mathtt{dom}(a) \rightarrowtail u$.

1. If $\mathtt{dom}(a) \not\rightarrowtail u$, then it follows from the definitions that $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\alpha a) = \mathtt{to}_u(\alpha')$, so by the inductive hypothesis, we have $s_0 \cdot \alpha \approx_u^{\mathtt{obs}} s_0 \cdot \alpha'$. By LR we moreover have $s_0 \cdot \alpha a \approx_u^{\mathtt{obs}} s_0 \cdot \alpha$, and we conclude $s_0 \cdot \alpha a \approx_u^{\mathtt{obs}} s_0 \cdot \alpha'$.
2. If $\mathtt{dom}(a) \rightarrowtail u$, then we may assume without loss of generality that $\alpha' = \beta b$ where $\mathtt{dom}(b) \rightarrowtail u$, else we may apply the previous case. It then follows from $\mathtt{to}_u(\alpha a) = \mathtt{to}_u(\beta b)$ that $a = b$ and $\mathtt{to}_u(\alpha) = \mathtt{to}_u(\beta)$ and $\mathtt{view}_{\mathtt{dom}(a)}(\alpha) = \mathtt{view}_{\mathtt{dom}(a)}(\beta)$. From the second of these facts, by the inductive hypothesis, we obtain $s_0 \cdot \alpha \approx_u^{\mathtt{obs}} s_0 \cdot \beta$. From the third, since the final observations of

the two views must be identical, we also have $s_0 \cdot \alpha \approx^{\mathtt{obs}}_{\mathtt{dom}(a)} s_0 \cdot \beta$. By WSC and $a = b$ we obtain $s_0 \cdot \alpha a \approx^{\mathtt{obs}}_{u} s_0 \cdot \beta b$, as required.

$\square$

5 Access Control Systems

As a particular application of the unwinding conditions, Rushby [Rus92] discusses a notion of access control system that he formulates in order to give semantic content to the Bell-La Padula model [BP76] (which has been criticised for lacking semantics). He shows that every access control system satisfying a compatibility condition with respect to a noninterference policy is IP-secure. In this section, we formulate a weaker variant of Rushby's definitions, and show that it implies the stronger notion of TA-security. We also show that our weaker variant implies the even stronger notion of TO-security, provided we work with a specific, but intuitive, definition of observation in access control systems.

Moreover, we also show a converse to the result that access control systems are TA-secure, viz., that every system satisfying TA-security can be interpreted as an access control system. This proves the *equivalence* in some sense of access control and TA-security. We believe that these results, together with the example of Section 3 and the results of the previous section, provide strong evidence that TA-security, rather than IP-security, is the notion that best realises the original objectives of the notion of intransitive noninterference.

According to Rushby, a *system with structured state* is a machine $\langle S, s_0, A, \mathtt{step}, \mathtt{obs}, \mathtt{dom}\rangle$ together with

1. a set N of *names*,
2. a set V of *values*, and functions
3. $\mathtt{contents} : S \times N \to V$, with $\mathtt{contents}(s, n)$ interpreted as the value of object n in state s,
4. $\mathtt{observe} : D \to \mathcal{P}(N)$, with $\mathtt{observe}(u)$ interpreted as the set of objects that domain u can observe, and
5. $\mathtt{alter} : D \to \mathcal{P}(N)$, with $\mathtt{alter}(u)$ interpreted as the set of objects whose values domain u is permitted to alter.

For a system with structured state, when $u \in D$ and s is a state, write $\mathtt{oc}_u(s)$ for the function mapping $\mathtt{observe}(u)$ to values, defined by $\mathtt{oc}_u(s)(n) = \mathtt{contents}(s, n)$ for $n \in \mathtt{observe}(u)$. Intuitively, $\mathtt{oc}_u(s)$ captures all the content of the state s that is observable to u. Using this, we may define a binary relation $\sim^{\mathtt{oc}}_u$ of *observable content equivalence* on S for each domain $u \in D$, by $s \sim^{\mathtt{oc}}_u t$ if $\mathtt{oc}_u(s) = \mathtt{oc}_u(t)$.

In order to capture the conditions under which the machine operates in accordance with the intuitive interpretations of this extra structure, Rushby defines the following three *Reference Monitor Assumptions*.

RM1. If $s \sim^{\mathtt{oc}}_u t$ then $\mathtt{obs}_u(s) = \mathtt{obs}_u(t)$.
RM2. If $s \sim^{\mathtt{oc}}_{dom(a)} t$ and either $\mathtt{contents}(s \cdot a, n) \neq \mathtt{contents}(s, n)$ or $\mathtt{contents}(t \cdot a, n) \neq \mathtt{contents}(t, n)$ then $\mathtt{contents}(s \cdot a, n) = \mathtt{contents}(t \cdot a, n)$

RM3. If $\texttt{contents}(s \cdot a, n) \neq \texttt{contents}(s, n)$ then $n \in \texttt{alter}(dom(a))$.

The first of these says that an agent's observation depends only on the values of the objects observable to the agent. The third says that if an action can change the value of an object, then the agent of that action is in fact permitted to alter that object. The condition RM2 is more subtle. The following provides a possibly more perspicuous formulation of this condition:

Proposition 8. *RM2 is equivalent to the following: For all states s, either*

1. *for all $t \sim^{\mathtt{oc}}_{dom(a)} s$, we have* $\texttt{contents}(t \cdot a, n) = \texttt{contents}(t, n)$, *or*
2. *for all $t \sim^{\mathtt{oc}}_{dom(a)} s$, we have* $\texttt{contents}(s \cdot a, n) = \texttt{contents}(t \cdot a, n)$

That is, with the choice depending only on information observable to $dom(a)$, the effect of the action is either to make no change to n or to assign a new value to n that depends only on information observable to $dom(a)$.

In addition to the reference monitor assumptions, Rushby considers the condition:

AOI. If $\texttt{alter}(u) \cap \texttt{observe}(v) \neq \emptyset$ then $u \rightarrowtail v$.

Intuitively, this says that the ability to write to a value that an agent can observe counts as a way to interfere with that agent. Rushby shows the following:

Proposition 9. *([Rus92], Theorems 2,8) Suppose M is a system with structured state that satisfies RM1-RM3 and AOI. Then the family of relations $\sim^{\mathtt{oc}}_{u}$ on M is a weak unwinding with respect to $\rightarrowtail$. Hence M is IP-secure for $\rightarrowtail$.*

By the results of the previous section, Rushby's result in fact yields the stronger conclusion that access control systems consistent with a policy are TA-secure. We can further strengthen this result by weakening the precondition.

Note that the condition RM2 says that the next value of n produced on performing an action a depends only on the values of names observable to $\texttt{dom}(a)$. If n is not observable to $\texttt{dom}(a)$, this may be too strong. Consider, for example, the situation where n represents a block of memory, and the action a writes to a single location within this block. Here the successor value depends on the value written (which will typically depend on the values of names observable to $\texttt{dom}(a)$), but also on the previous value of n. Similarly, if the name n is an object in an object-oriented system, and the effect of the action is to call a method of this object, then the successor value will depend of the input parameters of the call (which will depend on values of names observable to $\texttt{dom}(a)$), but also on the value of n. Thus, the condition RM2 can plausibly be weakened to the following.[3]

[3] A weakened condition resembling RM2$'$ has also been used in a slightly different context by Greve, Wilding and vanFleet [GWV03]. A similar weakening has also been proposed by von Oheimb [Ohe04], who also shows that the definition of access control system consistent with a policy can be weakened while still implying the existence

[RM2′] For all actions a, states s, t and names $n \in \texttt{alter}(dom(a))$, if $s \sim^{\texttt{oc}}_{\texttt{dom}(a)} t$ and $\texttt{contents}(s, n) = \texttt{contents}(t, n)$ we have $\texttt{contents}(s{\cdot}a, n) = \texttt{contents}(t \cdot a, n)$.

That is, for $n \in \texttt{alter}(dom(a))$, the value $\texttt{contents}(s \cdot a, n)$ is a function of both $\texttt{contents}(s, n)$ and $\texttt{oc}_{\texttt{dom}(a)}(s)$. Using Proposition 8 it can be seen that RM2 implies RM2′. The converse does not hold.

We now weaken Rushby's notion of access control system by replacing RM2 by RM2′. We define a system with structured states to be a *weak access control system* if it satisfies conditions RM1,RM2′, and RM3.

We also introduce a related notion on systems without structured states, that expresses that the system behaves as if it were an access control system. Say that a system M with states S *admits a weak access control implementation consistent with* $\rightarrowtail$ if there exists a set of names N, a set of values V and functions $\texttt{observe} : D \times S \to \mathcal{P}(N)$, $\texttt{alter} : D \times S \to \mathcal{P}(N)$ and $\texttt{contents} : N \times S \to V$, with respect to which M is a weak access control system satisfying the condition AOI.

The following shows that weak access control systems compatible with a policy satisfy Rushby's unwinding conditions for intransitive noninterference:

Proposition 10. *Suppose M is a weak access control system consistent with $\rightarrowtail$. Then the family of relations $\sim^{\texttt{oc}}_u$ is a weak unwinding on M with respect to $\rightarrowtail$.*

Proof. OC is direct from RM1 and LR follows easily from RM3 and AOI. For WSC, supppose that $s \sim^{\texttt{oc}}_{\texttt{dom}(a)} t$ and $s \sim^{\texttt{oc}}_u t$, i.e., $\texttt{oc}_u(s) = \texttt{oc}_u(t)$. We need to show $s \cdot a \sim^{\texttt{oc}}_u t \cdot a$, which amounts to showing $\texttt{contents}(s \cdot a, n) = \texttt{contents}(t \cdot a, n)$ for all $n \in \texttt{observe}(u)$. We consider the two possibilities $n \in \texttt{alter}(\texttt{dom}(a))$ and $n \notin \texttt{alter}(\texttt{dom}(a))$:

1. If $n \in \texttt{alter}(\texttt{dom}(a))$ then we have $\texttt{contents}(s \cdot a, n) = \texttt{contents}(t \cdot a, n)$ by RM2′.
2. If $n \notin \texttt{alter}(\texttt{dom}(a))$, then using RM3 we have $\texttt{contents}(s{\cdot}a, n) = \texttt{contents}(s, n) = \texttt{contents}(t, n) = \texttt{contents}(t \cdot a, n)$.

Thus, we have $s \cdot a \sim^{\texttt{oc}}_u t \cdot a$. □

We may also show a converse to this result, which leads to the conclusion that unwinding and weak access control systems are essentially equivalent.

---

of unwinding conditions implying IP-security. He adds the conditions $\texttt{dom}(a) \rightarrowtail u$, $n \in \texttt{observe}(u)$ and $s \sim^{\texttt{oc}}_u t$ to the antecedant of RM2. We would argue that there are some difficulties giving intuitive content to von Oheimb's proposal. First, whether or not a system is an access control system should be independent of the policy that may be applied to it. The fact $\texttt{dom}(a) \rightarrowtail u$ in the precondition is in any case derivable from $n \in \texttt{observe}(u)$ in the context of AOI and RM3, so can be omitted without loss of generality. Second, since u does not occur in the consequent, the quantification over u has a rather obscure meaning.

Proposition 11. *Suppose that there exists a weak unwinding on M with respect to $\rightarrowtail$. Then M admits a weak access control interpretation consistent with $\rightarrowtail$.*

Proof. Let the weak unwinding be $\{\sim_u\}_{u\in D}$. Write $[s]_u$ for the equivalence class of s under $\sim_u$. We define the access control interpretation on M as follows:

1. $N = D$
2. $\texttt{observe}(u) = \{u\}$
3. $\texttt{alter}(u) = \{v \in D \mid u \rightarrowtail v\}$
4. $\texttt{contents}(s, u) = [s]_u$.

Note that then $s \sim_u t$ iff $[s]_u = [t]_u$ iff $\texttt{contents}(s, u) = \texttt{contents}(t, u)$ iff $s \sim^{\texttt{oc}}_u t$.

RM1 is immediate from the fact that $\sim_u$ satisfies OC.

For RM2$'$, suppose that $n \in \texttt{alter}(\texttt{dom}(a))$ and $s \sim^{\texttt{oc}}_{\texttt{dom}(a)} t$ and $\texttt{contents}(s, n) = \texttt{contents}(t, n)$. Then $n \in D$, and from $\texttt{contents}(s, n) = \texttt{contents}(t, n)$ we get that $s \sim_n t$. From $s \sim^{\texttt{oc}}_{\texttt{dom}(a)} t$ we have that $s \sim_{\texttt{dom}(a)} t$. Hence by WSC, we have $s \cdot a \sim_n t \cdot a$, which is equivalent to $\texttt{contents}(s \cdot a, n) = \texttt{contents}(t \cdot a, n)$.

For RM3, we prove the contrapositive. Suppose that $n \notin \texttt{alter}(\texttt{dom}(a))$. Then $n \in D$ and $dom(a) \not\rightarrowtail n$. By LR, we have $s \cdot a \sim_n s$, which is equivalent to $\texttt{contents}(s \cdot a, n) = \texttt{contents}(s, n)$, as required.

Plainly, if $n \in \texttt{alter}(u)$ and $n \in \texttt{observe}(v)$ then $n = v$ and $u \rightarrowtail v$, so AOI also holds. □

Combining these results with those of the previous section, we see that there is a close correspondence between TA-security, weak access control interpretations, and weak unwindings.

Corollary 1. *The following are equivalent*

1. *M is TA-secure with respect to $\rightarrowtail$,*
2. *$\texttt{uf}(M)$ admits a weak access control interpretation consistent with $\rightarrowtail$,*
3. *there exists a weak unwinding on $\texttt{uf}(M)$ with respect to $\rightarrowtail$.*

Proof. The equivalence of (1) and (3) is from Theorem 3, and that between (2) and (3) follows from Propositions 10 and 11. □

From Theorem 2 and Proposition 10, we also obtain the following.

Corollary 2. *If M is a weak access control system consistent with $\rightarrowtail$ then M is TA-secure for $\rightarrowtail$.*

This conclusion is a more general result than Proposition 9, in which we have both weakened the antecedent and strengthened the consequent. The following example shows that we cannot further strengthen the conclusion to ITO-security.

Example 5. Consider the system for the policy $A \rightarrowtail B \rightarrowtail C$ with structured states for the set of names n_{AB}, n_{BC}, taking boolean values. Intuitively, these variables represent channels between the agents, so that $n_{AB} \in \texttt{alter}(A) \cap$

$\mathtt{observe}(B)$ and $n_{BC} \in \mathtt{alter}(B) \cap \mathtt{observe}(C)$. Plainly this is consistent with AOI. We represent states as tuples $s = (n_{AB}, n_{BC})$ with the obvious interpretation for `contents`. The initial state of the system is $(0, 0)$. Domain A has actions a with semantics $n_{AB} := 1$ and B has action b with semantics $n_{BC} := n_{AB}$. The observation functions are defined on the state $s = (n_{AB}, n_{BC})$ by $\mathtt{obs}_A(s) = \mathtt{obs}_B(s) = \bot$ and $\mathtt{obs}_C(s) = n_{BC}$. It can be verified that this system satisfies RM1,RM2$'$, RM3. However, it does not satisfy ITO-security. To see this, consider the sequences b and ab. Here we have

$$
\begin{aligned}
\mathtt{ito}_C(b) &= (\mathtt{ito}_C(\epsilon), \mathtt{view}_B(b), b) \\
&= (\mathtt{ito}_C(\epsilon), \bot b \bot, b) \\
&= (\mathtt{ito}_C(a), \mathtt{view}_B(ab), b) \\
&= \mathtt{ito}_C(ab)
\end{aligned}
$$

but $\mathtt{obs}_C(s_0 \cdot a) = 0 \neq 1 = \mathtt{obs}_C(s_0 \cdot ab)$. □

Notice that in this example, not all of the names observable to a domain have their contents visible in the observation of the domain. Say that a system with structured states is *fully observable* if in all states s we have $\mathtt{obs}_u(s) = \mathtt{oc}_u(s)$. Note that this means that the relations $\sim_u^{\mathtt{oc}}$ and $\approx_u^{\mathtt{obs}}$ coincide. We now obtain the following from Propositions 7 and 10. This shows that, modulo the reasonable assumption of full observability, we can derive a result similar to Corollary 2, but with the yet stronger conclusion of TO-security.

Corollary 3. *If M is a fully observable weak access control system consistent with $\rightarrowtail$ then M is TO-secure with respect to $\rightarrowtail$.*

A similar result does not hold with P-security in place of TO-security.

Example 6. Note that if in Example 5 we change the definition of $\mathtt{obs}_B(s)$ to n_{AB}, then the system continues to satisfy RM1,RM2$'$,RM3 and AOI, and not P-security. The modified system has $\mathtt{obs}_u(s) = \mathtt{oc}_u(s)$ for all states s. (So it also satisfies TO-security.) □

6 Conclusion

Our results have left open a number of technical questions. We have shown that weak unwindings provide a complete proof technique for TA-security, but have not provided a complete technique for TO-security. The reason for this is that there is inherently no tractable set of conditions on the states of the system that characterizes TO-security. We will treat this topic in a followup paper [Mey07b] which deals with the complexity of the notions of security discussed in this paper.

Our discussion has concentrated on a semantic model in which observations are associated to states. Rushby [Rus92] also formulates a notion of IP-security on a model where instead of state observations, actions produce outputs, and proves similar results concerning unwinding and access control systems for this model. We treat the relationship between the two models in a companion paper

[Mey07a], where we formulate a set of security notions for the action-observed model and show how these are related to the state-observed model under a transformations from the former to the latter. We also consider mappings to CSP processes there, and relate the definitions discussed in this paper to Roscoe and Goldsmith's definitions on CSP processes.

Another area requiring investigation is the generalization of our definitions to nondeterministic systems and systems that are not input-enabled, as has been studied for IP-security by von Oheimb [Ohe04]. More generally, one could consider extensions to the richer semantic framework of process algebra.

Both the fact, as argued by RG, that the notion of (intransitive) noninterference on its own falls short of expressing the correctness properties of downgraders that they sought to capture, and the fact, as we have shown, that there are several plausible notions of noninterference for intransitive policies, suggests that the notion of noninterference policy expressed by a relation $\rightarrowtail$ on domains lacks expressiveness that will be required in applications. We believe further work on richer formats for the expression of causality and information flow policies is warranted. The approach we have followed in this paper, of comparing an agent's actual information to an intuitive concrete operational model of the maximal information that an agent is permitted to have and transmit, could well be useful in this enterprise.

The specific case of downgrading policies has received some recent attention. Chong and Myers [CM04] have proposed a flexible language that attaches downgrading conditions to data items. Mantel and Sands [MS04] have proposed to introduce a programming annotation for downgrading, enabling the programmer to explicitly mark regions of code that are permitted to violate a transitive policy. They apply a definition based on IP-security. Bossi et al [BPR04] develop a theory of downgrading grounded in bisimulation-based notions of unwinding. Sabelfeld and Sands [SS05] lay out some general principles and direction for research in this area. It would be of interest to reconsider these contributions in the light of our results in this paper.

References

[BP76] D.E. Bell and L.J. La Padula. Secure computer system: unified exposition and multics interpretation. Technical Report ESD-TR-75-306, Mitre Corporation, Bedford, M.A., March 1976.

[BPR04] A. Bossi, C. Piazza, and S. Rossi. Modelling downgrading in information flow security. In *Proc. IEEE Computer Security Foundations Workshop*, pages 187–201, 2004.

[CM04] S. Chong and A. C. Myers. Security policies for downgrading. In *11th ACM Conf. on Computer and Communications Security (CCS)*, Oct 2004.

[FG01] R. Focardi and R. Gorrieri. Classification of security properties (Part I: information flow). In R. Focardi and R. Gorrieri, editors, *Foundations of Security Analysis and Design, FOSAD 2000, Bertinoro, Italy, September 2000*, volume 2171 of *LNCS*, pages 331–396. Springer, 2001.

[FHMV95] R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi. *Reasoning About Knowledge.* MIT-Press, 1995.

[GM82] J.A. Goguen and J. Meseguer. Security policies and security models. In *Proc. IEEE Symp. on Security and Privacy*, pages 11–20, Oakland, 1982.

[GM84] J.A. Goguen and J. Meseguer. Unwinding and inference control. In *IEEE Symp. on Security and Privacy*, 1984.

[GWV03] D. Greve, M. Wilding, and M. Vanfleet. A separation kernel formal security policy. In *Proc. Fourth International Workshop on the ACL2 Theorem Prover and Its Applications*, 2003. Paper and associated proof scripts at `http://www.cs.utexas.edu/users/moore/acl2/workshop-2003/`.

[HALL+05] N.B. Hadj-Alouane, S. Lafrance, Feng Lin, J. Mullins, and M.M. Yeddes. On the verification of intransitive noninterference in multilevel security. *IEEE Trans. on Systems, Man and Cybernetics, Part B*, 35(5):948– 958, Oct. 2005.

[HY87] J.T. Haigh and W.D. Young. Extending the noninterference version of MLS for SAT. *IEEE Trans. on Software Engineering*, SE-13(2):141–150, Feb 1987.

[McC88] D. McCullough. Noninterference and the composability of security properties. In *Proc. IEEE Symp. on Security and Privacy*, pages 177–186, 1988.

[Mey07a] R. van der Meyden. A comparison of semantic models of intransitive noninterference. submitted for publication, copy at `http://www.cse.unsw.edu.au/~meyden`, Dec 2007.

[Mey07b] R. van der Meyden. The complexity of notions of intransitive noninterference. unpublished manuscript, 2007.

[MS04] H. Mantel and D. Sands. Controlled declassification based on intransitive noninterference. In *Proc. Asian Symp. on Programming Languages and Systems*, volume 3302 of *LNCS*, pages 129–145. Springer-Verlag, November 2004.

[MZ06] R. van der Meyden and C. Zhang. A comparison of semantic models for noninterference. In *Proc. Workshop on Formal Aspects of Security and Trust, Hamilton, Ontario, Canada,*, LNCS. Springer, August 2006. to appear, extended version at `http://www.cse.unsw.edu.au/~meyden/research/publications.html`.

[Ohe04] D. von Oheimb. Information flow control revisited: Noninfluence = Noninterference + Nonleakage. In *Computer Security – ESORICS 2004*, volume 3193 of *LNCS*, pages 225–243, 2004.

[RG99] A. W. Roscoe and M. H. Goldsmith. What is intransitive noninterference? In *IEEE Computer Security Foundations Workshop*, pages 228–238, 1999.

[Rus81] J. Rushby. Design and verification of secure systems. In *Proc. 8th Symposium on Operating Systems Principles*, pages 12–21, Asilomar CA, Dec 1981. (ACM Operating Systems Review, Vol 15, No. 1).

[Rus92] J. Rushby. Noninterference, transitivity, and channel-control security policies. Technical Report CSL-92-02, SRI International, Dec 1992.

[Rya01] P.Y. Ryan. Mathematical models of computer security. In R. Focardi and R. Gorrieri, editors, *Foundations of Security Analysis and Design, FOSAD 2000, Bertinoro, Italy, September 2000*, volume 2171 of *LNCS*, pages 1–62. Springer, 2001.

[SS05] Andrei Sabelfeld and David Sands. Dimensions and principles of declassification. In *Proceedings of the 18th IEEE Computer Security Foundations Workshop*, pages 255–269. IEEE Computer Society Press, 2005.

[Sut86] D. Sutherland. A model of information. In *Proc. 9th National Computer Security Conf.*, pages 175–183, 1986.

[WJ90] J. T. Wittbold and D. M. Johnson. Information flow in nondeterministic systems. In *IEEE Symposium on Security and Privacy*, pages 144–161, 1990.