Fundamenta Informaticae 120 (2012) 1–15
DOI 10.3233/FI-2012-755
IOS Press

Informational Analysis of Security and Integrity*

Damas P. Gruska†
Institute of Informatics, Comenius University
Mlynska dolina, 842 48 Bratislava, Slovakia
gruska@fmph.uniba.sk.

Abstract. Formalisms for analysis of systems of various nature specified by process algebras are proposed. They allow us to formalize security properties based on an absence of information flow and properties on system's integrity. Resulting properties are compared and discussed. We present also quantification of these properties by means of information theory.

Keywords: information flow, opacity, nested attackers, information theory

1. Introduction

We propose formalisms for analysis of systems of various nature specified by process algebras. They allow us to formalize security properties based on an absence of information flow and properties on system's integrity. The presented approach combines several ideas emerged from security theory as well as its applications. As regards security, first we exploit an idea of an absence of information flow between public and private system's behaviour (see [18]). This concept has been many times exploited in various formalism. In security property called Non-Deductibility on Composition (NDC for short, see [7]) it is assumed that system's actions are divided to private and public ones. An information flow between these two kinds of actions is expressed in the following way: a system has NDC property if for every high level user A (i.e. the one capable to perform only private i.e. high level actions), the low level view of the behaviour (seeing only public i.e. low level actions) of P is not modified (in terms of weak trace equivalence) by the presence of A. In our approach we exploit this idea but we will consider several intruders which are differently nested inside a system (as it was done in [10, 17]) and later we

*Work supported by the grant VEGA 1/1333/12.
†Address for correspondence: Institute of Informatics, Comenius University, Mlynska dolina, 842 48 Bratislava, Slovakia

will consider also arbitrary processes not only high level ones. In this way we can check, for example, quality of various firewalls on different system's layers with respect to possible Trojan horses, viruses, and other suspicious processes from given set V. As the next step will formalize the information flow by opacity (see [3]). Opacity seems to be more suitable for analysis of security and integrity if one needs to capture more complex information flow then just the flow between private and public actions by means of a detected/excluded occurrence of a private ones. Note that opacity was already exploited also for definitions of security properties for process algebras (see [14]) and by means of opacity a diagnosability (as a complementary concept to security) for P Systems (see [1]) has been defined.

Combining the above mentioned approaches we propose the formalisms for analysis of both: information flow security as well as integrity of systems. We define properties as *Nested Non-Deducibility, Diagnosable intruders, Strongly Diagnosable intruders, Diagnosability for processes, Strong diagnosability for processes, Intruders detectable by weak trace equivalence* and *Strong intruders detectable by a predicate*. These properties express different requirements for systems's security and integrity (different notions of information flow, different notion of sets of possible intruders, different notions of security holes).

In general, the proposed properties are undecidable but become decidable for some special cases. Note that same basic notions of the presented approach were already developed in [11]. Here we present a quantification of these properties by means of information theory (see [12] for quantification of some (but much simpler) security properties for timed process algebras focused on so called timed attacks). In this way we can express how much information can be obtained about intruders or about system's security with respect to observations or we can express level of system's robustness with respect to its integrity.

Contribution. This work extends the previous works by the author: here we investigate and compare some security/integrity properties already suggested and we define and examine some new ones (Persistent Nested Non-Deducibility and some detectability properties). Note, that originally the name "diagnosability" appeared in the context of analysis of biological systems ([1]) and we have decided to keep the name also in this context. Moreover, here we study several different ways how to quantify presented security/integrity properties. We exploit techniques already developed for simpler security properties as well as we suggest new ones.

Organization of the paper. In Section 2 we describe Context process algebra (CTA, for short) which will be used as a basic formalism. In Section 3 we present and investigate the notion of diagnosability of intruders. Section 4 is devoted to quantification of diagnosability and in Section 5 we present and investigate other variants of diagnosability.

2. Context Process Algebra

In this section we define our working formalism - contexts process algebra (CPA). It is based on Milner's CCS (see [20]) which is extended by placeholders to specify processes contexts. To define the language CPA, we first assume a set of atomic action symbols A not containing symbols τ, and such that for every $a \in A$ there exists $\overline{a} \in A$ and $\overline{\overline{a}} = a$. We define $Act = A \cup \{\tau\}$. We assume that $a, b, \ldots$ range

over A and $x, y, \ldots$ range over Act. Assume the signature $\Sigma = \Sigma_0 \cup \Sigma_1 \cup \Sigma_2$, where

$$\begin{aligned}\Sigma_0 &= \{Nil\}\\ \Sigma_1 &= \{x. \mid x \in Act\} \cup \{[S] \mid S \text{ is a relabeling function}\}\\ &\quad \cup \{\backslash M \mid M \subseteq A\}\\ \Sigma_2 &= \{|, +\}\end{aligned}$$

with the agreement to write unary action operators in prefix form, the unary operators $[S], \backslash M$ in postfix form, and the rest of operators in infix form. Relabeling functions, $S : Act \to Act$ are such that $\overline{S(a)} = S(\bar{a})$ for $a \in A$, and $S(\tau) = \tau$.

The set of CPA terms over the signature Σ is defined by the following BNF notation:

$$P \ ::= \ X \ \mid \ \mathcal{A} \ \mid \ op(P_1, P_2, \ldots P_n) \ \mid \ \mu X P$$

where $X \in Var$, Var is a set of process variables, $\mathcal{A} \in PH$, PH is a set of process placeholders, $P, P_1, \ldots P_n$ are CPA terms, $\mu X-$ is the binding construct, $op \in \Sigma$. The set of CPA processes consists of closed CPA terms. The set of CCS processes consists of CPA processes without placeholders.

Let P be a CPA process with (all) placeholders $\mathcal{A}_1, \ldots, \mathcal{A}_n$. We will indicate this by $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$. CCS process obtained from from $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ by replacing placeholders $\mathcal{A}_i$ by CCS processes A_i will be indicated by $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n]$. Note that Nil will be often omitted from processes descriptions and hence, for example, instead of $a.b.Nil$ we will write just $a.b$. A structural operational semantics for CPA terms is given by means of labeled transition systems basicly the same as the one for CCS (see [20]).

For $s = x_1.x_2.\ldots.x_n, x_i \in Act$ we write $P \xrightarrow{s}$ instead of $P \xrightarrow{x_1}\xrightarrow{x_2} \cdots \xrightarrow{x_n}$ and we say that s is a trace of P. The set of all traces of P will be denoted by $Tr(P)$. By ϵ we will denote the empty sequence of actions, by $Succ(P)$ we will denote the set of all successors of P and $Sort(P) = \{x | P \xrightarrow{s.x}$ for some $s \in Act^\star$ and $x \neq \tau\}$. If the set $Succ(P)$ is finite we say that P is finite state. In the later we will use the weak trace equivalence and bisimulation.

Definition 2.1. The set of weak traces of process P is defined as $Tr_w(P) = \{s \in (A \cup \{t\})^\star | \exists P'.P \stackrel{s}{\Rightarrow} P'\}$. Two process P and Q are weakly trace equivalent ($P \approx_w Q$) iff $Tr_w(P) = Tr_w(Q)$. We say that process P is t-simulated by process Q ($P \preceq_w Q$) iff $Tr_w(P) \subseteq Tr_w(Q)$.

Definition 2.2. Let (CCS, $Act, \to$) be a labelled transition system (LTS). A relation $\Re \subseteq$ CCS $\times$ CCS is called a *bisimulation* if it is symmetric and it satisfies the following condition: if $P \Re Q$ and $P \xrightarrow{x} P', x \in Act$, then there exists a process Q' such that $Q \xrightarrow{x} Q'$ and $P' \Re Q'$. Two processes P, Q are *bisimilar*, abbreviated $P \sim Q$, if there exists a strong bisimulation relating P and Q.

Let us have a system described by CCS process P. Suppose that there are places in the system where an intruder or intruders can be put. We indicate those places by placeholders and the resulting CPA process will be called its opening. The opening of process can be defined on syntactical or semantical level. For simplicity we will use the later one.

Definition 2.3. Let P be a CCS process. Opening of P is any CPA process $Q[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ such that $P \sim Q[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil]$.

3. Diagnosable intruders

The first inspiration for our work is the security property Non-Deducibility on Composition (NDC for short, see in [7]). Suppose that all actions are divided in two groups, namely public (low level) actions L and private (high level) actions H i.e. $A = L \cup H, L \cap H = \emptyset$. Then process P has property NDC if for every high level user A, the low level view of the behaviour of P is not modified (in terms of weak trace equivalence) by the presence of A. The idea of NDC can be formulated as follows.

Definition 3.1. (NDC) $P \in NDC$ iff for every $A, Sort(A) \subseteq H \cup \{\tau\}$

$$(P|A) \setminus H \approx_w P \setminus H.$$

Note that in the case of NDC, only one attacker is considered and it communicates with the system on the top most level (non-nested attacker) and the system with and without the attacker are compared on level of weak traces. Our formalism of context process algebra allows us to model several intruders which can be nested arbitrary inside the system. In style of NDC we could define nested non-deducibility.

Definition 3.2. Let P be CPA process. We say that P has a property Nested Non-Deducibility ($P \in$ NND, for short) if

$$P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \setminus H \approx_w P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \setminus H$$

for every $A_i, Sort(A_i) \subseteq H \cup \{\tau\}, 1 \leq i \leq n$.

Example 3.3. In general we have $NND \subseteq NDC$ since clearly NDC is a special case of NND property. Let $P = l_1.Nil + (h.l_2.Nil) \setminus H$ It is easy to check that $P \in NDC$ but $P \notin NND$. Hence we have that $NND \subset NDC$.

The following lemma is preparation for the next proposition which allows us to restrict investigation of all possible high processed required by definition of NND.

Lemma 3.4. Let P be CPA process and let $A_i \preceq_w A'_i$, for $A_i, A'_i, Sort(A_i) \cup Sort(A\_i) \subseteq H \cup \{\tau\}, 1 \leq i \leq n$. Let Then we have $P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \setminus H \approx_w P[\mathcal{A}_1/A'_1, \ldots, \mathcal{A}_n/A'_n] \setminus H$ implies $P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \setminus H \approx_w P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \setminus H$.

Proof:
Clearly we have $Tr_w(P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \setminus H) \subseteq Tr_w(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \setminus H) \subseteq Tr_w(P[\mathcal{A}_1/A'_1, \ldots, \mathcal{A}_n/A'_n] \setminus H)$. □

As a consequence of the previous Lemma we have the following Proposition. It says that instead of checking all possible $A_i, Sort(A_i) \subseteq H \cup \{\tau\}$ it is enough to check so called the most powerful process Top (see also [7]).

Proposition 3.5. Let $P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \setminus H \approx_w P'[\mathcal{A}_1/Top, \ldots, \mathcal{A}_n/Top] \setminus H$ for CPA process P and $Top = \mu X \sum_{x \in H} h.X$. Then $P \in NND$.

In [6] Focardi and Rossi defined a security property which allows to deal systems "being secure in every state". We can reformulate this concept for NND property.

Definition 3.6. (Persistent NND) CPA process P has property *persistent NND* ($P \in$ PNND) iff $Succ(P) \subseteq$ NND

Note that clearly we have PNND $\subseteq$ NND. The following example shows that the inclusion is proper.

Example 3.7. Let $P = \tau.l.Nil + \tau.(\bar{h}.l.Nil|\mathcal{A})$. We have that $P \in$ NND but for $P' \in Succ(P), P' = (\bar{h}.l.Nil|\mathcal{A})$ we have $P' \notin$ NND and hence $P \in$ PNND.

The definitions of persistent PNND properties contain two universal quantifications (over all possible intruders and successors). To avoid both of them (quantification over intruders can be done as in Proposition 3.5) we exploit an idea introduced by Bossi, Focardi, Piazza and Rossi ([2]). First we introduce a low level observation equivalence (with respect to relation $\asymp$) which relates processes indistinguishable from the low level point of view.

Definition 3.8. (Equivalence on Low Actions) Let $\asymp$ be an equivalence relation over processes. We say that two processes P and Q are $\asymp$-equivalent on low actions, denoted by $P \asymp^l Q$, if $P \setminus H \asymp Q \setminus H$.

Now we can recall a notion of generalized unwinding condition. Roughly speaking, it requires that each high level action can be "simulated" in such a way that it is impossible for a low level user to infer which high level actions have been performed. All high level actions are required to be simulated in a way which is transparent to a low level user.

Definition 3.9. (Generalized Unwinding) Let $\asymp$ be an equivalence relation and $\longmapsto$ be a binary relation on processes. The unwinding class $(\mathcal{W}, \asymp^l, \longmapsto)$ is defined as $(\mathcal{W}, \asymp^l, \longmapsto) = \{P \in CPA | \forall Q \in Succ(P)$ if $Q \stackrel{h}{\rightarrow} R$ then $\exists R'$ such that $Q \longmapsto R'$ and $R \asymp^l R'\}$.

Theorem 3.10. Let $P \in (\mathcal{W}, \approx^l_w, \stackrel{\hat{\tau}}{\Rightarrow})$. Then it holds $P \in$ PNND.

Proof:
Let $P \in (\mathcal{W}, \approx^l_w, \stackrel{\hat{\tau}}{\Rightarrow})$ and let $P' \in Succ(P)$. It is enough to show that $Tr_w(P'[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \backslash H)$ $\subseteq Tr_w(P'[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \setminus H)$. Let $w \in Tr_w(P'[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \setminus H)$ be the shortest trace such that $w \notin Tr_w(P'[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \setminus H)$. Last element of w has to be a low level action l. This action is performed by P' itself (note that $Sort(A_i) \subseteq H \cup \{\tau\}$) before this action there should be a private action h such that this action is performed as a communication with some of A_i. But since $P \in (\mathcal{W}, \approx^l_w, \stackrel{\hat{\tau}}{\Rightarrow})$ this action could by "hide" by τ action(s) and resulting processes have to be in $\approx^l_w$ what is contradiction. □

Note that the inverse of the previous does not hold in general. It would hold for such processes for which a placeholder is put on the top most level within parallel operator $(P|\mathcal{A})$.

Now we will introduce several modifications of NND property. We begin with generalization of NND property by considering arbitrary nested processes and a general form of process opening i.e. no restriction operator has to be applied. While NDC and NND properties express that processes are secure for high level processes now we can express an integrity feature. In this way, we can check, for example, quality of various firewalls on different layers of system description with respect to possible Trojan horses, viruses, and other suspicious processes from given set V.

Definition 3.11. (Intruders detectable by weak trace equivalence)
Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We say that the intruders V are *detectable by weak trace equivalence* if

$$P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \not\approx_w P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n].$$

We will denote this by $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DT_V$.

The previous property can be seen as a generalization of NDC and NND properties as it is stated in the following lemma.

Lemma 3.12. $P \in NDC$ iff $(P|\mathcal{A}) \setminus H \notin DT_V$ for V such that $V = \{A|sort(A) \subseteq H \cup \{\tau\}\}$. $P \in NND$ iff $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \setminus H \notin DT_V$ for V such that $V = \{A_i|sort(A) \subseteq H \cup \{\tau\}, 1 \leq i \leq n\}$.

Proof:
If process P has NDC property than an observer can distinguish between an absence and presence of an intruder A such that $sort(A) \subseteq H \cup \{\tau\}$ by weak trace equivalence i.e. such the intruder is not detectable. The proof for NND is similar. □

Now we will generalize an idea of NND property by techniques similar to the ones developed for intruders diagnosability. Instead of CPA processes we consider CCS processes and all possible places where intruders or other suspicious processes from given set V could occur.

Definition 3.13. (Strong detectable by weak trace equivalence)
Given CCS process P and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We say that the intruders V are *strongly detectable by weak trace equivalence* if for every opening $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ of P it holds

$$P'[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil]) \not\approx_w P'[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n].$$

We will denote this by $P \in SDT_V$.

Proposition 3.14. $NND \subset (SDT_V)^c$ for every $V, V = \{A_1, \ldots, A_n\}, Sort(A_i) \subseteq H \cup \{\tau\}$, where $(SDT_V)^c$ is the set complement of SDT_V.

Proof:
Suppose that $P \in NND$. This means that a presence of nested intruders cannot be detected by an observer i.e. P does not belong to $(SDT_V)^c$ for every $V, V = \{A_1, \ldots, A_n\}, Sort(A_i) \subseteq H \cup \{\tau\}$. □

Above defined security properties would be appropriate in the case that an attacker can place several auxiliary processes inside the system in such a way that they can cause some information flow between private and public actions. But in many occasions division of actions to two static groups (one type of actions cannot be observed and another one is always observed) is not appropriate. Hence instead of variants of Non-Deducibility on Composition we will exploit more general concept opacity (see [3]). First we define observation function $\mathcal{O}$ on sequences from $Act^\star$ as function $\mathcal{O} : Act^\star \to \Theta^\star$ where Θ be a set of elements called observables. An observation function expresses what an observer - eavesdropper

can see from a system behaviour and we will alternatively use both the terms (observation - observer) with the same meaning.

Now suppose that we have some security property. This might be an execution of one or more classified actions, an execution of actions in a particular classified order which should be kept hidden, etc. Suppose that this property is expressed by predicate ϕ over process traces. Now we would like to know whether an observer can deduce the validity of the property ϕ just by observing sequences of actions from $Act^\star$ performed by given process. The observer cannot deduce the validity of ϕ for P if for every trace w of P such that $\phi(w)$ holds, there exists trace w' such that $\neg\phi(w')$ and the traces cannot be distinguished by an observer (see Fig. 1). We formalize this concept by opacity.

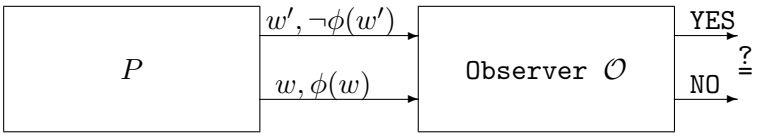

Figure 1. Opacity observer

Definition 3.15. (Opacity)
Given process P, a predicate ϕ over $Act^\star$ is opaque w.r.t. the observation function $\mathcal{O}$ if for every sequence w, $w \in Tr(P)$ such that $\phi(w)$ holds and $\mathcal{O}(w) \neq \epsilon$, there exists a sequence w', $w' \in Tr(P)$ such that $\neg\phi(w')$ holds and $\mathcal{O}(w) = \mathcal{O}(w')$. The set of processes for which the predicate ϕ is opaque with respect to $\mathcal{O}$ will be denoted by $Op^{\phi}_{\mathcal{O}}$.

The notion of opacity is rather general. With its help many other security properties can be defined (anonymity, non-interference etc. see [3]). On the other side, opacity is undecidable even for the simplest possible observation function, namely for the constant one, and for finite state processes (see [16]).

Now we are ready to to define diagnosability of intruders as a complementary property to opacity. We start with some notation. For CCS process P we will write $\phi(P)$ iff there exists $w, w \in Tr(P)$ such that $\phi(w)$ and we write $\phi^o(P)$ iff there exists $w, w \in Tr(P)$ such that $\phi(w)$ and $\mathcal{O}(w) = o$.

Definition 3.16. (Diagnosable intruders)
Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We say that the intruders V are *diagnosable* by a predicate ϕ over $Act^\star$ and by the observation function $\mathcal{O}$ if $\phi(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n])$ and $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \notin Op^{\phi}_{\mathcal{O}}$. We will denote this by $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_{V}$.

Example 3.17. Let us consider CPA process $P = ((h.l_1.Nil + l_2.Nil)|\mathcal{A}) \setminus \{h\}$, $\mathcal{O}(l_1) = \mathcal{O}(l_2) = l$, $\mathcal{O}(h) = \mathcal{O}(\tau) = \epsilon$ and $\phi(s)$ holds if s contains l_2. Then $P \notin DI^{\phi,\mathcal{O}}_{h.Nil}$ and $P \in DI^{\phi,\mathcal{O}}_{h.Nil}$.

Opacity, as it is defined in Definition 3.15, could be criticized from the both side - as a qualitative property it might happen that sometimes it is too weak or that in other cases it can be too strong. The same holds for diagnosability of intruders as it is clear from in the following example.

Example 3.18. Let us consider process

$$P^n = \sum_{i=1}^{2^k} h_i.(\sum_{j=1, j\neq n}^{2^k} l_j.\bar{l}_{refused} + l_n.\bar{l}_{accepted})$$

and CPA process $P = (P^n|\mathcal{A}) \setminus \{h_1, \ldots, h_{2^k}\}$. $\mathcal{O}(\tau) = \epsilon$, $\mathcal{O}(x) = x$ for other actions, and predicate ϕ_i such that $\phi_i(s)$ holds iff s contains action $l_{accepted}$. Let $A_i = \bar{h}_i.Nil$. Then $P \notin DI_{A_i}^{\phi,\mathcal{O}}$ iff $i = n$. In other words detectable are only such intruders which "know" secrete password h_n if we consider process P_n as a simple access control process. If k is large number, i.e. there are many possible passwords, then the probability that action $l_{accepted}$ is performed is very low i.e. probability to diagnose an intruder knowing the password ($h_n.Nil$) is also very low.

To overcame an insufficiency of (qualitative) diagnosability illustrated in the previous examples we will define quantitative measure of it.

4. Quantification of diagnosability

To define quantification of diagnosability we need some preparatory work. First we recall some basic concepts of information theory. To express quantity of information flow we will exploit Shannon information theory (see [22]). Let X be a discrete random variable and let x ranges over the set of values which X may take. By $p(x)$ we will denote probability that X takes the value x. Self-information (or surprisal) is a measure of the information content associated with the outcome of the random variable X. It is defined as $\mathcal{H}(x) = \log_b \frac{1}{p(x)}$. We put $\mathcal{H}(x) = \infty$ if $p(x) = 0$. The information entropy (also called self-information or a measure of uncertainty) of the variable X is denoted $\mathcal{H}(X)$ and is defined as $\mathcal{H}(X) = \sum_x p(x).\log_b \frac{1}{p(x)}$. We define $p(x).\log_b \frac{1}{p(x)} = 0$ if $p(x) = 0$. We will work with the base b of $\log_b$ equal to 2 and hence the unit of the information entropy will be one bit. Sometimes we will write $\mathcal{H}(p_1, \ldots, p_n)$ instead of $\mathcal{H}(X)$ if probabilities of values of X are $p_1, \ldots, p_n$. Given two random variables X and Y, the mutual information between them, written $\mathcal{I}(X;Y)$, is defined as $\mathcal{I}(X;Y) = \sum_x \sum_y p(x,y).\log \frac{p(x,y)}{p(x).p(y)}$.

4.1. Surprisal and uncertainty of security properties

To exploit information theory we need a way how to express probability of some observations. We will denote a multiset of finite traces of P by $MTr(P)$. For example, the trace $a.b$ is contained in $MTr(a.bNil + a.b.c.Nil)$ two times. There exist a few techniques how to define this multiset, originally developed for probabilistic process algebras (but here we will assume that all sequences have the same probability). For example, in [21] a technique of schedulers are used to resolve the nondeterminism and in [8] all transitions are indexed and hence pathes can be distinguished by different indexes. In the former case, every scheduler defines (schedules) a particular computation path and hence two different schedulers determine different pathes, in the later case, the index records which transition was chosen in the case of several possibilities. The set of indexes for process P consists of sequences $i_1 \ldots i_k$ where $i_j \in \{0,1,2\} \cup \{0,1,2\} \times \{0,1,2\}$. An index records how a computation path of P could be derived, i.e. it records which process was chosen in case of nondeterminism. If there is only one possible successor then transitions are indexed by 1 (i.e. corresponding $i_l = 1$) If transition $P \xrightarrow{x}$

P' is indexed by k (i.e. corresponding $i_l = k$) then transition $P + Q \xrightarrow{x} P'$ is indexed by $k.1$ and transition $Q + P \xrightarrow{x} P'$ is indexed by $k.2$. If transitions $P \xrightarrow{x} P'$ and $Q \xrightarrow{x} Q'$ are indexed by k and l, respectively, then transitions of $P|Q$ have indexes from $\{(k,0),(0,l),(k,l)\}$ depending on which transition rule for the parallel composition was applied. Every index defines at most one trace and the set of all indexes defines the multisets of traces $MTr(P)$. First we express quantification of an amount of information flow by means of the simplest concepts and later we develop more elaborated ones. Let $\mathcal{O}$ be an observation function and ϕ be a predicate over traces. Let $o \in Act^\star$. We denote $MTr(P)^{\mathcal{O}=o} = \{s | s \in MTr(P), \mathcal{O}(s) = o\}$ and $MTr(P)^{\mathcal{O}=o}_\phi = \{s | s \in MTr(P), \phi(s) \wedge (\mathcal{O}(s) = o)\}$. We define

$$p(MTr(P)^o_\phi) = |MTr(P)^{\mathcal{O}=o}_\phi| / |MTr(P)^{\mathcal{O}=o}|.$$

Definition 4.1. Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ and a set V, $V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We define surprisal $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi)$ of ϕ for process P, intruders V and observation $o, o \neq \epsilon$ as

$$\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) = \log \frac{1}{p(MTr(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n])^{\mathcal{O}=o}_\phi)}.$$

Example 4.2. 3.18 Let us consider CPA process P^n from Example 3.18 and $V = \sum_{i=1}^{2^k} \bar{h}_i.Nil$ and $o = l_{accepted}$. Then $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) = k$.

As it is stated in the following theorem there is a correspondence between a value of $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi)$ and predicate opacity and so surprisal can be seen as a quantification of opacity.

Theorem 4.3. $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_V$ iff $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) = 0$ for every o such that $\mathcal{O}(o) \neq \epsilon$ and $\phi^o(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n])$ where $V = \{A_1, \ldots, A_n\}$.

Proof:
Let $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_V$ and let $w \in Tr(P[\mathcal{A}_1, \ldots, \mathcal{A}_n])$ such that $\phi(w)$ and $\mathcal{O}(w) = o, o \neq \epsilon$. Then there does not exist w', $w' \in Tr(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n])$ such that $\neg\phi(w')$ and $\mathcal{O}(w) = \mathcal{O}(w')$. From this we have $p(MTr(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n])^{\mathcal{O}=o}_\phi) = 1$ i.e. $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) = 0$.

Let $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) = 0$ for every o such that $\mathcal{O}(o) \neq \epsilon$ and let $w \in Tr(P)$ such that $\phi(w)$ and $\mathcal{O}(w) = o$. Since $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) = 0$ we have that $p(MTr(P[\mathcal{A}_1, \ldots, \mathcal{A}_n])^{\mathcal{O}=o}_\phi) = 1$ i.e. there does not exist w', $w' \in Tr(P[\mathcal{A}_1, \ldots, \mathcal{A}_n])$ such that $\neg\phi(w')$ and $\mathcal{O}(w) = \mathcal{O}(w')$ i.e. $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \in DI^{\phi,\mathcal{O}}_V$. □

So if $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) = 0$ then from observation o we have certainty that for corresponding trace(s) of P predicate ϕ holds. If $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) \geq 1$ then it is equally or more probable that ϕ does not hold than it holds.

For nondeterministic choice of processes we have the following compositionality property.

Proposition 4.4. Let $V = \{A_1, \ldots, A_n\}$ and $\mathcal{H}(P[V]^{\mathcal{O}=o}_\phi) = e_1$, $\mathcal{H}(Q[V]^{\mathcal{O}=o}_\phi) = e_2$ then

$$\min\{e_1, e_2\} \leq \mathcal{H}((P+Q)[V]^{\mathcal{O}=o}_\phi) \leq \max\{e_1, e_2\}.$$

Proof:
Let $|MTr(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])^{\mathcal{O}=o}_{\phi}| = n_1$, $|MTr(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])^{\mathcal{O}=o}| = m_1$ and $|MTr(Q[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])^{\mathcal{O}=o}_{\phi}| = n_2$, $|MTr(Q[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])^{o}| = m_2$. Without loss of generality we can assume that $e_1 \leq e_2$ i.e. $n_1/m_1 \leq n_2/m_2$. From that we have $n_1.m_2 \leq n_2.m_1$. We have that $|MTr(P+Q)[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n]^{\mathcal{O}=o}_{\phi}| = n_1+n_2$ and $|MTr(P+Q)[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n]^{\mathcal{O}=o}| = m_1+m_2$ and so $n_1/m_1 \leq (n_1+n_2)/(m_1+m_2) \leq n_2/m_2$. □

The definition of predicate opacity (see Definition 3.15) is asymmetric in the sense that if $\phi(w)$ does not hold than it is not required that there exist another trace for which it holds (in general $Op^{\phi}_{\mathcal{O}} \neq Op^{\neg\phi}_{\mathcal{O}}$). This means that opacity says something to an intruder which tries to detect only validity of ϕ (if it is opaque, than validity cannot be detected) but not its non-validity i.e. it says nothing about predicate $\neg\phi$. The same hold for intruder's diagnosability.

To overcome this disadvantage we introduce a measure of uncertainty of ϕ under observation o. The uncertainty expresses an amount of information which can be learned by attacker about predicate ϕ.

Definition 4.5. Given CPA process $P[\mathcal{A}_1,\ldots,\mathcal{A}_n]$ and a set V, $V = \{A_1,\ldots,A_n\}$ of CCS processes called intruders (we will write $P[V]$ instead of $P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n]$). We define uncertainty $\mathcal{H}_u(P[V]^{\mathcal{O}=o}_{\phi})$ of ϕ for process P and observation $o, o \neq \epsilon$ as $\mathcal{H}_u(P[V]^{\mathcal{O}=o}_{\phi}) = p(MTr(P[V])^{\mathcal{O}=o}_{\phi}).\log\frac{1}{p(MTr(P[V])^{\mathcal{O}=o}_{\phi})} + (1-p(MTr(P[V])^{\mathcal{O}=o}_{\phi})).\log\frac{1}{1-p(MTr(P[V])^{\mathcal{O}=o}_{\phi})}$.

The uncertainty expresses how uncertain is predicate ϕ under observation o. The maximal value (equal to 1) means that probabilities that ϕ holds and that ϕ does not hold are equal. The uncertainty has a similar relationship to opacity as the surprisal (see Theorem 4.3). Also the proof is similar.

Proposition 4.6. If $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_V$ then $\mathcal{H}_u(P[V]^{\mathcal{O}=o}_{\phi}) = 0$ for every o such that $\mathcal{O}(o) \neq \epsilon$ where $V = \{A_1,\ldots,A_n\}$.

The inverse implication in Proposition 4.6 does not hold but we have the following property. Its proof is straightforward.

Proposition 4.7. If $\mathcal{H}_u(P[V]^{\mathcal{O}=o}_{\phi}) = 0$ for every o such that $\mathcal{O}(o) \neq \epsilon$ where $V = \{A_1,\ldots,A_n\}$ then $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI^{\phi,\mathcal{O}}_V$ or $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI^{\neg\phi,\mathcal{O}}_V$.

5. Variants of diagnosability

Property *Diagnosable intruders* suppose that we know the set V of intruders in advance. This is not always the case and hence we define a property, called *Strongly Diagnosable intruders*, which does not expect any set of intruders in advance. In this way we can specify, for example, a quality of strongest firewalls.

Definition 5.1. (Strongly Diagnosable intruders)
Given CPA process $P[\mathcal{A}_1,\ldots,\mathcal{A}_n]$. We say that the intruders are *strongly diagnosable* by a predicate ϕ over $Act^{\star}$ and by the observation function $\mathcal{O}$ for $P[\mathcal{A}_1,\ldots,\mathcal{A}_n]$ if there exists a set $V, V = \{A_1,\ldots,A_n\}$ of CCS processes such that it holds $\phi(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])$ and $P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n] \notin Op^{\phi}_{\mathcal{O}}$. We will denote this by $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in SDI^{\phi,\mathcal{O}}$.

A relationship between Strongly Diagnosable intruders and Diagnosable intruders is given by the following theorem.

Proposition 5.2. $SDI^{\phi,\mathcal{O}} = \bigcup_{V,V=\{A_1,\ldots,A_n\},A_i\in CCS} DI_V^{\phi,\mathcal{O}}$.

Proof:
Let us suppose that $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in SDI^{\phi,\mathcal{O}}$ then there exists a set $V, V = \{A_1,\ldots,A_n\}$ of CCS processes such $\phi(P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n])$ and $P[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n] \notin Op_{\mathcal{O}}^{\phi}$. From this we have $P[\mathcal{A}_1,\ldots,\mathcal{A}_n] \in DI_V^{\phi,\mathcal{O}}$. The proof of the inverse inclusion is similar. □

Diagnosability of intruders assumes also that we know possible holes (placeholders in our formalism) for the intruders in a system specification (as CPA term) and a set of intruders. This is not always the case and hence we define diagnosability for CCS processes (see for comparison Definition 3.13 of Strong detectable by weak trace equivalence).

Definition 5.3. (Diagnosability for processes)
Given CCS process P and a set $V, V = \{A_1,\ldots,A_n\}$ of CCS processes called intruders. We say that the processes V are *strongly diagnosable processes* by a predicate ϕ over $Act^\star$ and by the observation function $\mathcal{O}$ if for every opening every P' of P it holds $P'[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n]) \notin Op_{\mathcal{O}}^{\phi}$. We will denote this by $P[V] \in DP_V^{\phi,\mathcal{O}}$.

A relationship between Diagnosable intruders and Diagnosability for processes is given by the following theorem.

Proposition 5.4. $P \in DP_V^{\phi,\mathcal{O}}$ iff $P'[\mathcal{A}_1/A_1,\ldots,\mathcal{A}_n/A_n] \in DI_V^{\phi,\mathcal{O}}$ for every opening P' of P.

Proof:
The proof follows directly from Definition 2.3 and 5.3. □

No we are ready to define the most general of the previous notions, called *Strong diagnosability for processes*, which does not assume that either a possible set of intruders (V) is known in advance nor possible placing of these intruders (placeholders). This property generalize the two above defined properties.

Definition 5.5. (Strong diagnosability for processes)
Given CCS process P and the observation function $\mathcal{O}$. We say that P is strongly diagnosable by a predicate ϕ over $Act^\star$ if there exists a set V such that V is strongly diagnosable by ϕ and $\mathcal{O}$. We will denote this by $\in SDP^{\phi,\mathcal{O}}$.

Proposition 5.6. $P \in SDP^{\phi,\mathcal{O}}$ iff $P' \in SDI^{\phi,\mathcal{O}}$ for every opening P' of P.

Proof:
The proof follows directly from Definition 2.3 and 5.5. □

As it is clear from the previous theorems that the above mentioned properties have different strengths as regards diagnosability as well as their complements have different strengths as security properties. Now we will quantify these properties.

Definition 5.7. Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$. We define strong surprisal $\mathcal{H}^s(P[V]_\phi^{\mathcal{O}=o})$ of ϕ for process P as

$$\mathcal{H}^s(P_\phi^{\mathcal{O}=o}) = \min\{\mathcal{H}(P[V]_\phi^{\mathcal{O}=o}) | V = \{A_1, \ldots, A_n\}, A_i \in CCS\}.$$

¿From Theorem 4.3 we know that if $\mathcal{H}^s(P_\phi^{\mathcal{O}=o}) = 0$ then there exist intruders $A_1, \ldots, A_n$ which are diagnosable for $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$, ϕ and $\mathcal{O}$.

Definition 5.8. Given CCS process P and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We define process surprisal $\mathcal{H}^p(P[V]_\phi^{\mathcal{O}=o})$ of ϕ for intruders V and observation $o, o \neq \epsilon$ as

$$\mathcal{H}^p(P[V]_\phi^{\mathcal{O}=o}) = \min\{\mathcal{H}(P'[V]_\phi^{\mathcal{O}=o}) | \text{ where } P' \text{ is an openning of } P\}.$$

Again, if $\mathcal{H}^p(P[V]_\phi^{\mathcal{O}=o}) = 0$ then there exists an opening P' of P such that intruders $V = \{A_1, \ldots, A_n\}$ are diagnosable by ϕ and $\mathcal{O}$.

Definition 5.9. Given CCS process P. We define strong process surprisal $\mathcal{H}^{sp}(P_\phi^{\mathcal{O}=o})$ of ϕ for process P and observation $o, o \neq \epsilon$ as

$$\begin{aligned} \mathcal{H}^{sp}(P_\phi^{\mathcal{O}=o}) \quad = \quad & \min\{\mathcal{H}(P'[V]_\phi^{\mathcal{O}=o}) | V = \{A_1, \ldots A_n\}, A_i \in CCS \\ & \text{and } P' \text{ is an opening of } P\}. \end{aligned}$$

If $\mathcal{H}^{sp}(P_\phi^{\mathcal{O}=o}) = 0$ then there exists such an opening P' of P and intruders $V = \{A_1, \ldots, A_n\}$ they they are diagnosable by ϕ and $\mathcal{O}$.

As a consequence of theorems 5.2, 5.4 and 5.6 we get the following corollary.

Corollary Let P be a CCS process, $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ its opening and $V, V = \{A_1, \ldots, A_n\}$ be CCS processes . Then it holds

$$\mathcal{H}^{sp}(P_\phi^{\mathcal{O}=o}) \leq \mathcal{H}^s({P'}_\phi^{\mathcal{O}=o}) \leq \mathcal{H}(P'[V]_\phi^{\mathcal{O}=o}).$$

Now, at the end we will return to modifications of NDC and NND properties.

Definition 5.10. (Intruders detectable by a predicate)
Given CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ and a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes called intruders. We say that the intruders V are *detectable* by a predicate ϕ over $Act^\star$ and by the observation function $\mathcal{O}$ for $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$ if $P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n] \notin Op_\mathcal{O}^\phi$ but $P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil] \in Op_\mathcal{O}^\phi$. We will denote this by $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DT_V^{\phi,\mathcal{O}}$.

In general, properties *Intruders detectable by a predicate* and *Intruders detectable by weak trace equivalence* correspond to different detectability approaches and represent different observational power as well as different requirement on a property we are looking for.

Proposition 5.11. There exist CPA processes $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$, $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n]$, a set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes, a predicate ϕ over $Act^\star$ and an observation function $\mathcal{O}$ such that $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DT_V^{\phi,\mathcal{O}}$, $P[\mathcal{A}_1, \ldots, \mathcal{A}_n] \notin DT_V$ and $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n] \notin DT_V^{\phi,\mathcal{O}}$, $P'[\mathcal{A}_1, \ldots, \mathcal{A}_n] \in DT_V$.

Proof:
Let us consider $V = \{h.Nil\}$, predicate ϕ for which $\phi(s)$ holds if $h_1 \in s$ and $\mathcal{O}(h_1) = \mathcal{O}(h) = \mathcal{O}(\tau) = \tau$ and $\mathcal{O}(x) = x$ otherwise. Now let us consider CPA process $P = ((h_1.l.Nil + \bar{h}.l.Nil)|\mathcal{A}) \setminus \{h\}$. Now we check that $P \in DT_V^{\phi,\mathcal{O}}$ but $P \in DT_V$. If we consider CPA process $P' = ((h_1.l.Nil + \tau.l.Nil + \bar{h}.h_1.l.Nil)|\mathcal{A}) \setminus \{h\}$ then we can check that $P \notin DT_V^{\phi,\mathcal{O}}$ but $P \notin DT_V$. □

Example 5.12. Let us consider $V = \{h.Nil\}$, predicate ϕ for which $\phi(s)$ holds if $h_1 \in s$ and $\mathcal{O}(h_1) = \mathcal{O}(h) = \mathcal{O}(\tau) = \tau$. Now let us consider CPA process $P = ((\tau.\tau.Nil + \tau.h_1.Nil + \bar{h}.h_1.\tau.Nil)|\mathcal{A}) \setminus \{h\}$. It can be checked that $P \in DT_V^{\phi,\mathcal{O}} \cap DT_V$. This, together with Theorem 5.11, give us a general relation between $DT_V^{\phi,\mathcal{O}}$ and DT_V for given V, ϕ and $\mathcal{O}$ (see Fig. 2).

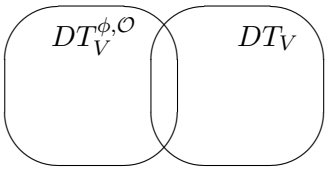

Figure 2. $DT_V^{\phi,\mathcal{O}}$ vs. $\in DT_V$

We can quantify property "Intruders detectable by a predicate" in the following way. Let us consider CPA process $P[\mathcal{A}_1, \ldots, \mathcal{A}_n]$, set $V, V = \{A_1, \ldots, A_n\}$ of CCS processes, a set of observations O and two random variables V_O and N_O which express for every $o \in O$ probability (as they are exploited in Definition 4.1) that it $\phi(s)$ and $\phi(s')$ hold, for $\mathcal{O}(s) = \mathcal{O}(s') = o$ where $s \in MTr(P[\mathcal{A}_1/A_1, \ldots, \mathcal{A}_n/A_n]$ and $s' \in MTr(P[\mathcal{A}_1/Nil, \ldots, \mathcal{A}_n/Nil]$, respectively. We define the mutual information between V_O and N_O as follows

$$\mathcal{F}(V_O \rightsquigarrow N_O) = \mathcal{I}(V_O, N_O).$$

Higher values of $\mathcal{F}(V_O \rightsquigarrow N_O)$ indicate stronger detectibility by predicate. In a similar way we could naturally quantify also other above mentioned properties. Since security properties are complementary to detectability ones we get in this way also their quantification.

6. Discussion

We have presented several formalisms for analysis of systems of various nature specified by process algebras. They combine several information flow based security notions and approaches and they allow us to formalize such properties of systems as diagnosability, detection ability and a presence of, for example, intruders and other suspicious software components. Some of resulting properties can be viewed as complementary to security ones.

Traditional security properties and hence also our starting formalisms, which are somehow based on them, are frequently criticized of being either too strong or to weak what is a direct consequence of they qualitative nature. So we have developed their quantitative variants. The quantification is made by means of information theory. In this way we can express levels of system's security and integrity.

For the sake of simplicity we have worked with classical process algebra instead of a probabilistic process algebra (depending on an application one can chose between reactive, generative or stratified probabilistic calculi, see [8]). Using that kind of algebras we could have more adequate tools for expressing probabilities of traces. Instead of that we have used uniform probability distribution but all the concepts and results could be easily translated to a probabilistic calculus. Actually we would have different definitions of $p(MTr(P)^o_\phi)$ which appears in Definition 4.1 and 4.5 of surprisal and uncertainty and it would influence also the definition of mutual information flow ($\mathcal{F}(V_O \rightsquigarrow N_O)$).

As regards the future work, besides considering probabilistic process algebra, we plan to investigate changes of a level of security of process P by putting it to different contexts and by composing it with other processes. We plan to formalize also unprecise observations. We can model this by observational functions which map every trace of actions to a discrete random variable which ranges over strings from $\Theta^\star$. Moreover we can associate some probability distribution to resulting possible observations for a given "unprecise" observer. For example, we can model Gaussian (or any other) distribution of errors for different kinds of observation etc.

References

[1] Barbuti R., D.P. Gruska, A. Maggiolo-Schettini and P. Milazzo: A notion of biological diagnosability inspired by the notion of opacity in systems security. Fundamenta Informaticae, Vol. 102, No. 1 (2010), s. 19-34, 2010.

[2] Bossi A., R. Focardi, C. Piazza and S. Rossi. Refinement Operators and Information Flow Security. Proc. of SEFM'03, IEEE Computer Society Press, 2003.

[3] Bryans J., M. Koutny, L. Mazare and P. Ryan: Opacity Generalised to Transition Systems. In Proceedings of the Formal Aspects in Security and Trust, LNCS 3866, Springer, Berlin, 2006.

[4] Clark D., S. Hunt and P. Malacaria: A Static Analysis for Quantifying the Information Flow in a Simple Imperative Programming Language. The Journal of Computer Security, 15(3). 2007.

[5] Focardi, R., R. Gorrieri, and F. Martinelli: Information flow analysis in a discrete-time process algebra. Proc. 13^{th} Computer Security Foundation Workshop, IEEE Computer Society Press, 2000.

[6] Focardi, R. and S. Rossi: Information flow security in Dynamic Contexts. Proc. of the IEEE Computer Security Foundations Workshop, 307-319, IEEE Computer Society Press, 2002.

[7] Focardi, R., R. Gorrieri, and F. Martinelli: Real-Time information flow analysis. IEEE Journal on Selected Areas in Communications 21 (2003).

[8] Glabbeek R. J. van, S. A. Smolka and B. Steffen: Reactive, Generative and Stratified Models of Probabilistic Processes Inf. Comput. 121(1): 59-80, 1995.

[9] Gorrieri R. and F. Martinelli: A simple framework for real-time cryptographic protocol analysis with compositional proof rules. Science of Computer Programming archive Volume 50, Issue 1-3, 2004.

[10] Gorrieri R., F. Martinelli and I. Matteucci: Specification and Analysis of Information Flow Properties for Distributed Systems. Submitted for publications, 2010.

[11] Diagnosability of nested intruders, Proc. of Bionetics 2010, Springer Verlag, 2010.

[12] Gruska D.P.: Quantifying Security for Timed Process Algebras Fundamenta Informaticae, Vol. 93, No. 1-3, 2009.

[13] Gruska D.P.: Probabilistic information flow security. Fundamenta Informaticae, Vol. 85, No. 1-4, 2008.

[14] Gruska D.P.: Observation Based System Security. Fundamenta Informaticae, vol 79, Numbers 3-4, 2007.

[15] Gruska D.P.: Information-Flow Security for Restricted Attackers. in Proc. of 8th International Symposium on Systems and Information Security, Sao Jose dos Campos, 2006.

[16] Gruska D.P.: Information Flow in Timing Attacks. Proceedings CS&P'04, 2004.

[17] Gruska D.P. and A. Maggiolo-Schettini: Nested Timing Attacks, in proceedings of FAST'03, Pisa, pp 147-161, 2003.

[18] Goguen J.A. and J. Meseguer: Security policies and security models. Proc. of IEEE Symposium on Security and Privacy, 1982.

[19] Lowe G.: Quantifying information flow". In Proc. IEEE Computer Security Foundations Workshop, 2002.

[20] Milner, R.: *Communication and concurrency.* Prentice-Hall International, New York, 1989.

[21] Segala R. and N. Lynch: Probabilistic Simulations for Probabilistic Processes. Nord. J. Comput. 2(2): 250-273, 1995.

[22] Shannon, C. E.: A mathematical theory of communication. Bell System Technical Journal, vol. 27, 1948.