RESEARCH PAPERS OF WROCŁAW UNIVERSITY OF ECONOMICS
No. 85 2009
Advanced Information Technologies for Management – AITM 2009

Ernesto Damiani[(1)], Gabriele Gianini[(1)], Florian Kerschbaum[(2)], Richard Pibernik[(3)]

[(1)] Università degli Studi di Milano, [(2)] SAP Research, [(3)] European Business School

TOWARD VALUE-BASED CONTROL OF KNOWLEDGE SHARING IN NETWORKED SERVICES DESIGN

Abstract: The notion of cooperative, service-based processes is a crucial one for achieving high flexibility in designing and deploying inter-organizational business applications. However, inter-organizational business processes are known to be prone to a number of security risks. Research on secure distributed computing has traditionally focused on attacks delivered by outsiders; but a major source of risk for business processes is hostile or dysfunctional behaviour of insiders. In particular, the sharing of knowledge that inevitably takes place in cooperative business processes is a major source of risk, as selfish or malicious actors can extract knowledge from the process' information flows they have access to and use it for their own advantage. This *disclosure risk* depends on the specific business process and on the value of disclosed information, which changes over time. In this work, we outline the definition of a framework supporting process-driven assessment of information value and value-based definition of a disclosure risk: this framework enables process designers to dynamically compute orchestrations that minimize the risk of knowledge disclosure while minimizing the orchestration's own cost, in the presence of changing information value and both rational and malicious actors.

1. Introduction

In the context of business process design, risk has been considered mainly from a project-management perspective; however, risk is an inherent property of every business process. Furthermore, while security research has traditionally focused on outsider attacks, it is now recognized that a major source of business risk in cooperative business processes is due to dysfunctional behaviour of insiders, i.e. individuals or organizations taking part in the process. From a purely rational standpoint, dysfunctional behaviour on the part of insiders takes place when cooperating delivers a lower payoff than defecting or adopting any other type of non-cooperative behaviour.

In turn, this payoff depends on the specific business process economics and on the value of disclosed information, which changes over time. In the past, much research work has been done on analyzing the risk of running business processes either in the presence of purely rational (selfish) participating entities (actors) or in the presence of

irrational, malicious actors: the first case requires a game-theoretical approach where one needs to provide incentives for the rational nodes to prevent them from disclosing information (as they act upon their self-interest); the second case has been studied by the distributed computing research community, which has proposed robust protocols to alleviate the effect of malicious behaviour. Those models fit the behaviours of both individuals and organizations: typically organizations will mostly act rationally, i.e. they may disclose information learned of a process' task due to their economic self-interest (they may obtain more benefit from not collaborating); individuals (who act on behalf of organizations) will, instead, sometimes act rationally, but some other times can decide to attack without apparent reason (e.g., disgruntled employees who just want to harm the outcome of the process).

In this paper, we argue that it is possible for business process designers to dynamically compute business orchestrations that minimize the risk of knowledge disclosure while minimizing the orchestration's own cost, in the presence of (i) changing information value, and (ii) both rational and malicious actors. A methodological advantage of disclosure risk analysis is that one can derive the value of disclosed information from the business process model, without any additional modelling of security solutions.

In this paper we outline the foundational elements of a theoretical framework – called NADIR (*kNowledge Assets and DIsclosure-Risk aware re-design*) – supporting the process-driven assessment of information value, the value-based definition of a knowledge disclosure risk and the design of an information disclosure risk aware re-orchestration.

NADIR includes a hybrid analysis based on process economics as well as the users' subjective perceptions in order to compute the business process dynamic risk landscape. Based on the latter it is possible to compute sets of access rules to the knowledge items exchanged during a business process. These rule sets are then used to compute secure business process orchestrations able to guarantee (under certain conditions) that rational (selfish) actors have incentives to stay with the process and at the same time, alleviate the negative impact of actions by malicious nodes.

Business processes are normally secured by applying operational security solutions (such as encryption and access control rules) to existing orchestrations. NADIR provides a novel approach to securing business processes using risk estimates to suggest how to re-orchestrate business processes, providing the business process designer with valuable alternatives.

The paper is organized as follows: first we recall some foundational elements of the economics of knowledge and information and point to other contributions from the areas of distributed system engineering, ICT security and risk management where the NADIR methodology is grounded (Section 2); then we outline our methodology (Section 3) and point out its innovative aspects with respect to the state of the art (Section 4).

2. Related work

2.1. Knowledge and information economics

Knowledge can be considered as a resource that a business can use in production, alongside physical capital, labour/human capital, and other inputs. Originating from the strategic management literature, this perspective extends the resource-based view of the firm [Penrose 1959;Wernerfelt 1984; Barney et al. 2001; Conner 1991]. Indeed, knowledge is no ordinary product: unlike tangible goods, it is embedded and carried through multiple entities including organizational culture and identity, policies, routines, documents, systems, and employees. Knowledge is *non-rival* (consuming some information does not exclude someone else from also consuming the same information). Furthermore, unlike ordinary products and services, knowledge does not have the basic property of *exclusion*: if something is known, it is difficult and costly to exclude others from its use. Due to its special status, knowledge cannot be dealt with by standard economic theories. Nevertheless, in the context of the manufacturing and service industries knowledge has a business value, determined by several factors. One factor is related to the market value of the goods and services produced by the organization holding the knowledge; another factor is the number of actors that share it.

Those two factors are in turn controlled by two opposing mechanisms: on the one hand, knowledge *sharing* can help leveraging the collaborative creation of higher quality goods and services (some scholars stress the capability of hierarchical organizations in facilitating knowledge transfer [Arrow 1974; Kogut, Zander 1992, 1996; Nahapiet, Ghoshal 1998], emphasizing the firms' capacity to support the formation of a shared language and environment for collaboration); on the other hand, *exclusion* from knowledge can safeguard individuals' and organizations' knowledge assets.

Indeed, due to the relative easiness by which knowledge objects can be reproduced and communicated the value of the knowledge can significantly *change over time* in correspondence of acts of knowledge communication and transfer. Opportunistic behaviour (and its preventions) is recognized as one of the determinants of the structure of organizations [Foss 1996; Heiman, Nickerson 2002; Williamson 1999]. Opportunistic behaviours can include appropriation of knowledge; indeed some scholars emphasize the role of organizations, specifically of hierarchical organizations, in avoiding knowledge transfer [Demsetz 1988; Conner 1991, Conner, Prahalad 1996]. In both points of view, however, the value of the knowledge owned by an actor or by an organization is time-dependent.

2.2. ICT security

Knowledge intensive business processes involve normally the execution of coordination protocols on an ICT infrastructure, which can be represented by a

network of nodes. In an ideal situation the nodes taking part to the protocol may try to maximize the overall *common good* of the community, i.e. their objectives may be aligned. In practice, however, nodes may rather behave selfishly, looking out for their own interest. In this case the objectives of the different players will not be aligned, and it will be possible to analyze the probable strategies in view of conflicting interests from a rational standpoint by using the theory of *non-cooperative games*.

When rationality cannot always be assumed, e.g. in Collaborative Peer-to-Peer Computing (CP2PC), alternative approaches have been proposed relying on reputation and trust feedback mechanisms [Damiani et al. 2003]. CP2PC has been studied from two different points of view: a "classical" distributed computing view [Fernandez et al. 2006; Konwar et al. 2006] and a game-theoretic one [Fernandez et al. 2008; Yurkewych et al. 2005]. From the first point of view, the actors are classified as either malicious or correct, based on a predefined behaviour: the malicious actors show a "dysfunctional" behaviour due to a software error or when the actor intentionally behaves maliciously. From the game-theoretic point of view, actors act in their own self-interest, that is, they are assumed to be rational [Shneidman, Parkes 2003]: in other words, actors decide on whether to be honest or to cheat depending on which strategy increases their benefit (utility). From this point of view, strategic games are used to quantify the necessary incentives so that the actors' interests are best served by acting "correctly". The design objective is forcing a desired Nash equilibrium [Nash 1950], i.e., a strategy choice by each actor such that none of them has incentive to change it unilaterally. At the Nash equilibrium point, one achieves the minimum level of risk while minimizing cost or satisfying a certain budget. However, the literature in this area focuses on collaborative aspects rather than on dysfunctional behaviour and its results concerning the understanding on how one can lessen the impact of malicious nodes in collaborative games are still preliminary [Mailath, Samuelson 2006]. A few recent works [Aiyer et al. 2005; Gairing 2008; Moscibroda et al. 2006] have considered both rational (selfish) and malicious nodes, but for very different problems and with very different goals.

2.3. Risk management

Generally speaking, a risk management framework is composed of three main action phases: identification, analysis and control. A way to frame risks in a precise fashion is to characterize them, using properties such as impact, probability, time frame and coupling with other risks [Gemmer 1997]. Four risk-handling strategies are suggested in the literature: *mitigation*, *avoidance*, *transfer* and *acceptance*/*assumption*. Risk transfer consists in shifting risk from one party to another (e.g. by insurance); risk avoidance consists in eliminating the probability of a specific risk before its occurrence (e.g. by a suitable process redesign); risk mitigation consists in reducing the probability of a risk and/or the impact that an occurrence of the risk may bear (e.g. by a suitable re-orchestration); risk acceptance/assumption refers to the act

of adapting to the risk when it becomes a problem (enactment of a risk contingency plan is required in this strategy). While risk avoidance and mitigation typically aim at reducing the probability of a given error, risk transfer and assumption consider more the magnitude of the error consequences. Our approach is aimed at risk avoidance and mitigation.

Techniques for securing business processes have so far focused on incorporating security technology, such as network cryptography [Backes et al. 2003] or separation-of-duty [Wolter, Schaad 2007], into existing business process modelling technology. The business process models are then refined in order to translate them into executable business processes. At this stage, one can specify additional assumptions regarding security, e.g. trust assumptions, similar to our information value. These modelling tools reduce the burden on the business process designer, since they allow automatic validation of the business process to the specification. The goal of our research is very different in respect to the category of threats targeted by our framework: information disclosure. Up to now, only a few works (see for instance [Damiani 2009]) have investigated the problem of taking into account the risk of dysfunctional behaviour when designing business processes. This risk however is even more relevant to business processes than the one of outsider's attacks. For cross-organizational business processes the threat of information disclosure significantly outweighs threats from attackers on the network, while for internal business processes the main menace is often represented by hostile behaviour by insiders. For instance, in the key application areas of new product development and supply chain management these disclosure risks are particularly important, since the information is of very high value to the competition.

3. The methodology

3.1. Outline of the NADIR approach

The approach of NADIR is grounded on the economics of knowledge, but is aimed at using economic analysis (together with security-inspired models of non-rational, dysfunctional behaviour) to carry out focused risk analysis at the level of individual business processes, leading to process-specific risk monitoring and, if needed, to risk-aware business process (re)design. NADIR analyzes business process design with the tools of game theory, identifying critical points in the process orchestration, related to the possible defection of individual actors. This analysis is based on the notion of *security invariants*, i.e., relations that link shared information value and disclosure payoff. A typical NADIR invariant is the one stating that "At each step of the process and for each actor A, the decrease in value of the knowledge items held by A must not be greater than A's expected payoff from correct process execution". The violation of a security invariant, like the one above, during process execution could trigger the defection of an actor (individual of organization).

Rational causes for dysfunctional behaviour can be integrated with indicators of the onset of non-rational dysfunctional behaviour, taking into account the difference between prevalently rational, corporate actors (e.g., modelling business partner organizations) and mostly irrational individual players, (e.g., modelling insider attackers like disgruntled employees). Once the evolving risk landscape of a business process has been identified followed along the process enactment, it is possible to use it to redesign the process economics introducing a suitable incentives system, or to redesign the process itself by acting over its orchestration, so as to control the spread of knowledge and its progressive change in value, thus making the process more robust to the possible dysfunctional behaviour of some actors. Indeed research has shown that, given a business process orchestration, one can derive a set of access control policies, which is minimal and necessary [Kerschbaum, Robinson 2009]: from this follows that a minimum risk orchestration can be stated as an access control policy on the knowledge items exchanged during the process. In turn – should the operational context require it – such access control policy can be stated either as a business process re-orchestration or in terms of a suitable encryption key distribution scheme [Kerschbaum, Robinson 2009].

This methodological approach can help business process designers in applying risk-aware process engineering techniques to specific knowledge intensive business processes. The lifecycle of the NADIR methodology is shown in Figure 1.

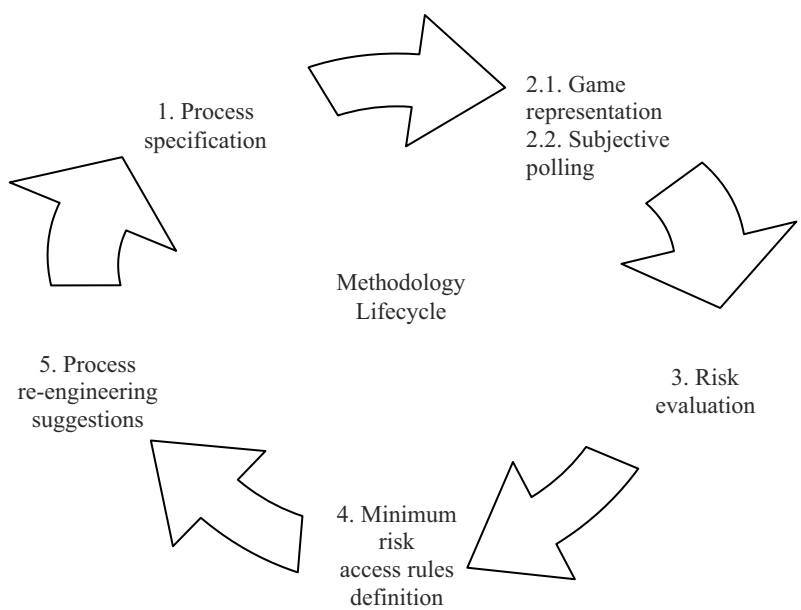

Figure 1. Schematic view of NADIR methodology lifecycle

Source: own elaboration.

Schematically the lifecycle consists in the following iterative processes.

1. The initial specification of the process under investigation is mapped into a representation suitable to game theoretical and distributed system analysis, which are at the basis of the economics-based risk analysis.

2. The economics-based risk analysis is then performed, based on the notion of *security invariants*, i.e., relations that link shared information value and disclosure payoff. In turn, the behaviour of malicious individuals (modelled as non-rational actors) is represented by super-imposing uncertainty (a probability) on rational behaviour. The superposition uses the value of information as perceived by the community (estimated by direct questions and probes) to modulate the probability of deviating from rational behaviour to non-rational malicious behaviour, typical of individuals. The output of the analysis is the probability of adverse events like insider attacks (defections, disclosures, etc.). An illustrative example of assessment of the probability dysfunctional behaviour based only on rational elements is given below.

3. Then computing the impact of the different adverse events allows dynamic quantification of the risk (computed as probability times impact), providing a dynamic risk landscape showing risk per-actor and per-knowledge item.

4. Based on the risk landscape, a set of security requirements can be defined. In the simplest case this can be a set of access rules minimizing the risk. Specifically NADIR derives a set of minimally necessary access rules that both, fulfil the purpose of the business process, and are acceptable by the risk assessment. The Minimum Risk Access Rule Definition step derives these rules from (parts of) the business process description and the risk evaluation. It is a well-known fact that there is a correspondence between access rules and business processes, namely that access rules can be derived from a business process description. These rules are minimal and necessary, i.e. removing an access right prevents the business process from running and adding an access right only increases the disclosure risk. It seems rather obvious that this transformation from business process to access rules loses information, i.e. there are multiple business processes that map to the same set of access rules. Many different algorithms have been developed for this conversion, including ones incorporating time [Kerschbaum, Robinson 2009].

5. The Process Re-engineering Suggestions step of NADIR enhances these methods with a well-designed reverse process that suggests a re-engineered business process for a given set of access rules. Namely, the NADIR methodology can suggest a business process alternative in case the risk evaluation concludes that the information disclosure risk of the current orchestration is unacceptable. Of course, security technology does not only offer access control as a means to control information disclosure. In some cases it may be acceptable from a risk perspective to disclose aggregate or derived information. NADIR investigates alternative, novel methods, such as usage policies or privacy-preserving computation, in order to control information disclosure. This can open a new alternative in business processes to the simple and obvious choice of "to disclose or not to disclose". An illustrative

example of re-orchestration which improves over an existing process design is given hereafter. The computational and organizational cost of implementing these solutions, such as trusted computing or secure computation, needs to be considered in relation to the gained benefit.

3.2. Value-based assessment of the probability of dysfunctional behaviour

In order to illustrate NADIR's novel approach to risk assessment we introduce a toy example referring to two actors participating into a sequential production process within an organization *O*. It is important to remark again that the NADIR risk assessment technique will put together rational and non-rational behaviour; but for the sake of simplicity in this example we shall outline rational, economics-based risk analysis only.

Let us assume that the organization *O* is a software producer and that it is outsourcing the execution of different tasks of the software production to actors which do not know each other and cannot communicate directly:

1) to actor *A* is assigned the role of performing task *a*, at time 1, say designing a software – on the basis of the requirements received in input – and producing the corresponding information item, a software detailed design blueprint,

2) to actor *B* is assigned the role of performing task *b*, at time 2, say implementing the software: he will produce the corresponding information item, the software code, in the form of a set of high-level programming language files and the corresponding executable binary code.

Subsequently the software will undergo other phases and eventually be commercialized and distributed in the form of binaries. However this will happen only at time 4, due to the latency of the overall procedure in the organization *O*. The two actors will obtain for the added value, contributed to the product, a market share equal to 10 thousand euro each. The process is repeated every time the organization *O* decides to produce a new software unit. Let us assume now that on the market there is a competitor organization *N*, and that the commercialized binary code of *O*'s product cannot be reverse-engineered effectively: the total value of the information items that *A* and B handle is greater than what they are going to receive for their added value. The competitor organization *N*, which is more efficient and has a shorter time-to-market than *O*, could secretly offer to each actor *A* and *B*, at time 2, a conspicuous amount of money for buying their information items, with the aim of commercializing the same product at time 3. In this way *N* would lock the market and leave no gain for organization *O*, which in turn would not have any market share to pay to actors *A* and *B*. The organization *N* has only a limited budget of 50 thousand to devote to this operation of intelligence. Furthermore it will have to formulate the deal to *A* and *B* through different undercover intermediaries in parallel, hence the amount will have to be split into two parts if both the actors accept the proposal and defect from *O*.

This leads to a situation where the two actors *A* and *B* – which we assume to be aware of the fact that *N* has contacted both, but not to be able to communicate to one another – to a strategic situation (the payoff for what a player chooses to do will depend also on what the other players do, and this holds for all players) depicted in the following table.

	Collaborate with *O*	Defect from *O*
Collaborate with *O*	10.10	0.50
Defect from *O*	50.0	20.30

One can readily recognize here an instance of the well-known Prisoner Dilemma (PD) game. Each player has two strategies available: Collaborate and Defect, each cell contains the payoffs for the two players corresponding to the combination of strategies (the first number represents the payoff for *A* the second the payoff for *B*). At first glance it might seem that the higher payoff to *B* in case of joint defection would make him more prone to defection; however if we consider fully rational actors this consideration does not apply, since if both are rational they will both Defect with certainty. Hereafter we will discuss how NADIR risk assessment will provide a different result, first with rational agents in a one round PD then for finitely iterated PD, and we will show how one gets a higher risk for *B*.

We considered actors as purely rational and pursuing the maximization of their own payoff then for each player the best strategy is the one specified by the Nash equilibrium of the game: the situation where no player would obtain a higher payoff by deviating unilaterally from it. In a single round Prisoner Dilemma, the Nash equilibrium is at the cell (Defect, Defect), because a player leaving unilaterally this point would lower his payoff. Notice that each player has here a payoff for joint collaboration $P = 10$, a reward for joint defection $R = 20$ or $R = 30$, a reward for unilateral defection $T = 50$, and a payoff for unilateral collaboration $S = 0$; however, the fact that the best strategy is "Defect" holds in general, provided that in the payoff matrix **M** for each player one has $T > P$ and $R > S$.

However the single round (*one-shot*) game is not realistic, as in a real organization the process of producing some product from scratch would normally be repeated several times; let us assume that the game will continue with further rounds even if one of the players has defected in previous ones. If the rational players know that the game will last exactly *n* rounds, then at round $(n - 1)$ the players face an ordinary one-shot PD, and they will defect: by induction the rational players deduce that they should defect at every step since the beginning. This phenomenon is called sometimes *backward induction "paradox"*, because it contrasts with substantial evidence from experimental economics showing that human players tend to cooperate faithfully in repeated interactions, especially in early periods when the end of the game is still far away [Szabo, Fáth 2007].

A common explanation is that players are not fully rational or that their rationality is not common knowledge: each player knows that he is rational, but perceives a chance that the co-players are not. This information asymmetry makes the game a different game – namely a finitely repeated game based on a stage game with incomplete information – and assures cooperation, provided that the game is long enough and the stage game payoffs satisfy some simple inequalities: the reason is that there is an incentive for rational players to mimic non-rational players and thus create a reputation (of being non-rational, i.e., cooperative) for which the other's best reply is cooperation, at least sufficiently far from the last stage.

NADIR game-theoretical approach focuses exactly on this point. Notice that each player can infer the other's move in the previous round from his own payoff at the end of that round: in these Iterated Prisoner Dilemmas (hence forth IPDs) players who defect in one round can be "punished" by defections in subsequent rounds and those who cooperate can be rewarded by cooperation. Of course, the number of possible strategies for deciding at each move whether to Collaborate or to Defect on the basis of the other player's moves in the previous rounds increases exponentially with the memory depth m kept by the player, but it is possible to formulate effective strategies which make use of limited resources, such as the *Tit-For-Tat* strategy (cooperation on the first round and imitation of the opponent's previous move thereafter). Kreps et al. [1982] provide a bound L on the number of rounds at which Defect may be played when at least one player is committed to a TFT strategy.

In the NADIR approach, the value of L depends on the expected payoffs from attack and cooperation. Extending the simple example above, these payoffs (i) *vary at each step of the business process* and (ii) *include the value of information held by each actor at each step of the process execution*.

At the light of point (ii), i.e. considering the fact that at each process step some knowledge is acquired and/or released, coming up with mathematically well-defined functions of time for these payoffs can be very difficult.

In general, however, we can safely assume that in most cases the knowledge value in a business process can be approximated by a stepwise descent, associated to knowledge communication/transfer events.

Note that knowledge transfer can be intentional – functional to the normal operation of one of the business process activities, like parameter passing to a remote service – or an unintentional event, due to information leakage, malicious inference or to the reverse engineering of the final product.

NADIR provides an empirical assessment of knowledge value as follows: at each step of the business process, each actor will see the value of her overall knowledge assets change due to (i) the "do-nothing" change to the value of the knowledge she already holds (typically a downward step change), and (ii) new knowledge acquired from other actors.

In NADIR, these rational arguments allow assessing from a rational standpoint the risk that at a given round of the game an actor will have already defected. This

assessment is made through the quantity L: the shorter L is, the sooner an actor is expected to defect.

In our toy example, the higher is defection payoff R, the shorter will be L; generally speaking, however, we can state that when the evolution of an actor's payoff for legitimate behaviour, *minus the decrease in the value of her knowledge*, brings it below the expected outcome of dysfunctional behaviour, the actor will be at high risk of defection with respect to correct business process execution.

In other words, at step i, the length of the cooperative streak will be estimated as

$$L_i = f(P_i - R_i - \Delta KV_i),$$

where P_i is the expected payoff of cooperation at time i, R_i is the expected payoff of defection at time i and ΔKV_i is the decrease due to step i of the value of the knowledge held by the actor, e.g. because the process step requires sending some information to other actors.

All other conditions being fixed, we consider that the higher is the reward in joint defection R_i for an actor, the more risky is the actor.

In our toy example, the NADIR-style risk ranking would indicate actor B as the most risky, and actor A as a less risky one, and for the sake of preventing disclosure attacks O's software development process should be enacted having this risk ranking in mind.

3.3. Risk-aware choice between competing orchestrations

We will provide now an illustrative example of risk-aware re-orchestration; for sake of simplicity we will consider a simple process admitting a small number of alterative orchestrations. Let us consider a business process where some information item, e.g. a document, held by an actor A, needs – in order to proceed in its processing – to be signed both by an actor B and by an actor C: both B and C can get hold of the information contained in the document. Suppose furthermore that, due to some process *external* to the one under focus, the value of information is progressively decreasing with time. Suppose each actor has an associated threshold value and that when the value of the item they handle exceeds that threshold they can adopt a dysfunctional behaviour (e.g. selling the information to outsiders) with some probability.

In a disclosure-risk unaware orchestration (*white board* orchestration), illustrated in Figure 3, actor A could send the document in parallel to both B and C and wait for both approvals to come back. However while A waits for the signature there would be three actors at risk of dysfunctional behaviour: although the value of the information item has decreased, at step 2 it is still above the three individual thresholds. In a disclosure-risk aware orchestration, on the other hand, one could play in a mitigation approach illustrated in Figure 4: A sends the document first to B and waits for

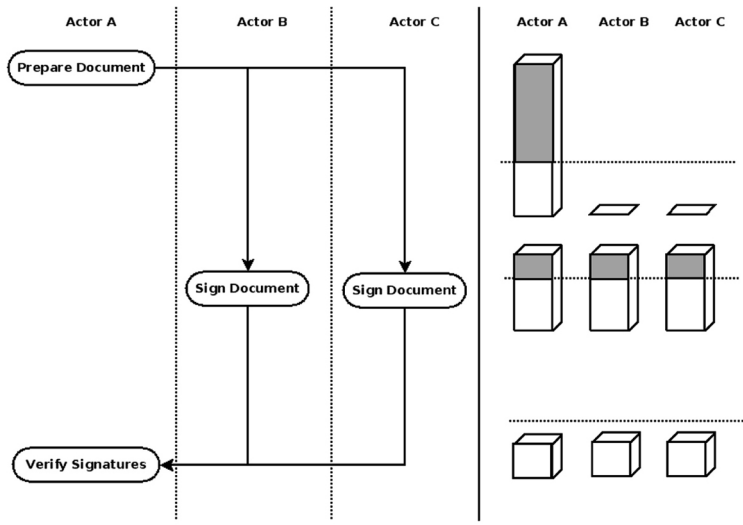

Figure 2. Illustration of a disclosure-risk unaware orchestration. On the left the activity diagram of the business process, on the right the parallel evolution of the information assets for the three actors: the value of information is progressively decreasing with time, due to external factors. The shaded area represents the amount by which, at each step, the information asset of an actor exceeds her individual threshold, making the actor at risk of dysfunctional behaviour. Notice that at step 2, according to this orchestration there are three actors at risk

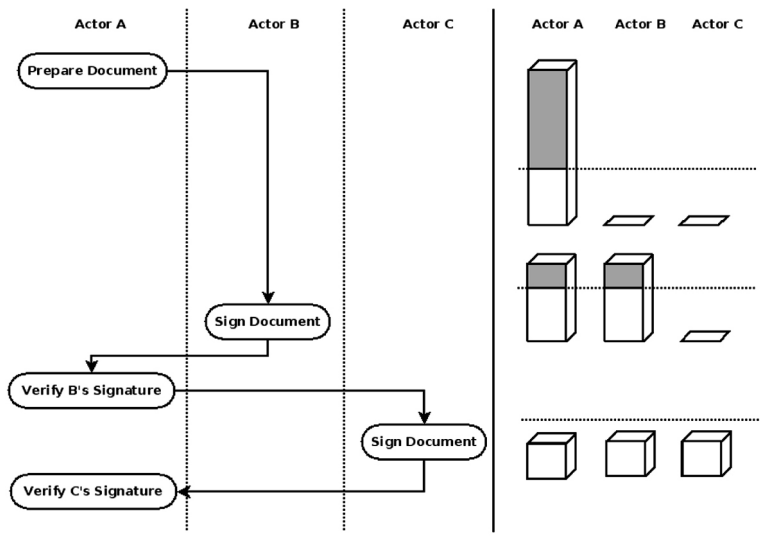

Figure 3. Illustration of a disclosure risk-aware orchestration.
Notice that at step 2, according to this orchestration there are only two actors at risk

approval, then *A* sends the document to *C* for final approval: in this way, at step 2 of the process only two actors are above the threshold of risk. *In this second orchestration there are never more than two actors at risk of dysfunctional behaviour.*

3.4. Modelling irrational behaviour

The above examples used an entirely rational standpoint for analysis. Indeed, the computer security approach – which models actors as functional units which may randomly adopt a dysfunctional behaviour – and the game theoretic approach used in economics studies – which models organizations as networks of interdependent rational (selfish) agents – have been used independently from each other.

NADIR integrates the two approaches via a probabilistic superposition: all agents are considered fully rational agents as in the examples above, but each agent has some uncertainty superimposed to its rational behaviour. This superposition results in hybridizing rational behaviour, typical of organizations, with non-rational malicious behaviour, typical of individuals.

In the hybridization technique we aim to take into account the difference between prevalently rational, corporate actors (e.g., modelling business partner organizations) and mostly irrational individual players, (e.g., modelling insider attackers like disgruntled employees): the probability of malicious attack by an actor will be subjective and depend on the community view of the value of the information she owns.

4. Conclusions

The economics of security is a hot and rapidly growing field of research: more and more researchers and practitioners are realizing that security failures are often due to security experts focusing on defences against hacking and intrusions without taking into account the economics behind malicious and dysfunctional behaviour of insiders and business partners. Some work has been done to use economics to drive security investments, as well as on using incentives as an alternative to conventional security techniques (a full-length survey paper is [Anderson, Moore 2006]). However, while economic analysis can provide some insight on mass phenomena that IT security researchers have found difficult to handle, it must still show that it can help to improve security solutions in company and, more importantly, in business-process-specific scenarios.

The NADIR framework aims to bring economic analysis into the toolkit of the business process designer and of the IT security expert. NADIR analysis builds on ongoing work on the role of information assets in organizations, and on the related risks, involving aspects of information economics (including key areas of game theory such as asymmetric information games), and integrating them with business process risk modelling and advanced modelling of the social aspects of collaborative networks.

References

Aiyer A.S., Alvisi L., Clement A., Dahlin M., Martin J., Porth C. (2005), BAR fault tolerance for cooperative services, [in:] *Proceedings of SIGOPS*, Operational Systems Review, Vol. 39, No. 5, pp. 45-58.

Anderson R., Moore T. (2006), The economics of information security, *Science*, Vol. 314, No. 5799, pp. 610-613.

Arrow K.J. (1974), *The Limits of Organization*, Norton and Co., New York.

Backes M., Pfitzmann B., Waidner M. (2003), Security in business process engineering, [in:] *Proceedings of the International Conference on Business Process Management, 2003 (BPM2003)*, Lecture Notes in Computer Science (LNCS), Vol. 2678, pp. 168-183.

Barney J., Wright M., Ketchen Jr D.J. (2001), The resource-based view of the firm: Ten years after 1991, *Journal of Management*, Vol. 27, No. 6, pp. 625-641.

Conner K.R. (1991), A historical comparison of resource-based theory and five schools of thought within industrial organization economics: Do we have a new theory of the firm?, *Journal of Management*, Vol. 17, No. 1, pp. 121-154.

Conner K.R., Prahalad C.K. (1996), A resource-based theory of the firm: knowledge versus opportunism, *Organization Science*, Vol. 7, No. 5, pp. 477-501.

Damiani E. (2009), Risk-aware collaborative processes, [in:] *ICEIS 2009 – Proceedings of the 11th International Conference on Enterprise Information Systems (DISI, Milan, Italy, 2009)*, pp. 29-29.

Damiani E., De Capitani Di Vimercati S., Paraboschi D., Samarati P. (2003), Managing and Sharing Servents' Reputations in P2P Systems, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 15, No. 4, pp. 840-854.

Demsetz H. (1988), The theory of the firm revisited, *Journal of Law Economics and Organization*, Vol. 4, No. 1, pp. 141-162.

Fernandez A., Lopez L., Santos A., Georgiou C. (2006), Reliably executing tasks in the presence of untrusted entities, [in:] *Proceedings of 25th IEEE Symposium on Reliable Distributed Systems (IEEE Computer Society 2006)*, pp. 39-50.

Fernandez A., Georgiou Ch., Mosteiro M.A. (2008), Designing mechanisms for reliable Internet-based computing, [in:] *Seventh IEEE International Symposium on Network Computing and Applications, 2008*, NCA '08 (IEEE Computer Society), pp. 315-324.

Foss N.J. (1996), Knowledge-based approaches to the theory of the firm: Some critical comments, *Organization Science*, Vol. 7, No. 5, pp. 470-476.

Gairing M. (2008), Malicious Bayesian congestion games, [in:] *Proceedings of WAOA 2008*, Lecture Notes in Computer Science (LNCS), Vol. 5426 (2009), pp. 119-132.

Gemmer A. (1997), Risk management: Moving beyond process, *Computer*, Vol. 30, pp. 33-43.

Heiman B., Nickerson J.A. (2002), Towards reconciling transaction cost economics and knowledge-based view of the firm: The context of interfirm collaboration, *International Journal of the Economics of Business*, Vol. 9, No. 1, pp. 97-116.

Kerschbaum F., Robinson P. (2009), Security architecture for virtual organizations of business web services, *Journal of Systems Architecture – Embedded Systems Design*, Vol. 55, No. 4, pp. 224-232.

Kogut B., Zander U. (1992), Knowledge of the firm, combinative capabilities and the replication of technology, *Organization Science*, Vol. 3, No. 3, pp. 383-397.

Kogut B., Zander U. (1996), What firms do? Coordination, identity, and learning, *Organization Science*, Vol. 7, No. 5, pp. 502-518.

Konwar K.M., Rajasekaran S., Shvartsman A.A. (2006), Robust network supercomputing with malicious processes, [in:] *Proceedings of DISC 2006*, Lecture Notes in Computer Science (LNCS), Vol. 4167, pp. 474-488.

Kreps D.M., Milgrom P., Roberts J., Wilson R. (1982), Rational cooperation in the finitely repeated Prisoner's Dilemma, *Journal of Economic Theory*, Vol. 27, pp. 245-252.

Mailath G., Samuelson L. (2006), *Repeated Games and Reputations: Long-run Relationships*, Oxford University Press, Oxford.

Moscibroda T., Schmid S., Wattenhofer R. (2006), When selfish meets evil: Byzantine players in a virus inoculation game, [in:] *Proceedings of the Twenty-Fifth Annual ACM Symposium on Principles of Distributed Computing (2006)* (ACM, New York, NY), pp. 35-44.

Nahapiet J., Ghoshal S. (1998), Social capital, intellectual capital, and organizational advantage, *Academy of Management Review*, Vol. 23, pp. 242-266.

Nash J.F. (1950), Equilibrium points in n-person games, *Proceedings of National Academy of Sciences of the United States of America*, Vol. 36, No. 1, pp. 48-49.

Penrose E.G. (1959), *The Theory of the Growth of the Firm*, Wiley, New York.

Shneidman J., Parkes D.C. (2003), Rationality and self-interest in P2P networks, [in:] *Proceedings of the Second International Workshop on Peer-to-Peer Systems (IPTPS 2003)*, Lecture Notes in Computer Science (LNCS), Vol. 2735, pp. 139-148.

Szabó G., Fáth G. (2007), Evolutionary games on graphs, *Physics Reports*, Vol. 446, pp. 97-216.

Wernerfelt B. (1984), A resource-based view of the firm, *Strategic Management Journal*, Vol. 5, No. 2, pp. 171-180.

Williamson O.E. (1999), Strategy research: Governance and competence perspectives, *Strategic Management Journal*, Vol. 20, No. 12 (Dec., 1999), pp. 1087-1108.

Wolter Ch., Schaad A. (2007), Modelling of task-based authorization constraints in BPMN, [in:] *Proceedings of the International Conference on Business Process Management, 2007*, Lecture Notes in Computer Science (LNCS), Vol. 4714, pp. 64-79.

Yurkewych M., Levine B.N., Rosenberg A.L. (2005), On the cost-ineffectiveness of redundancy in commercial P2P computing, [in:] *Proceedings of the 12th ACM Conference on Computer and Communications Security, CCS 2005*, (ACM), pp. 280-288.