Salim, Farzad and Reid, Jason and Dulleck, Uwe and Dawson, Edward (2010) *Towards a game theoretic authorisation model.* In: Conference on Decision and Game Theory for Security (GameSec 2010), 22-23 November 2010, Berlin, Germany. (In Press)

Towards a Game Theoretic Authorisation Model

Farzad Salim[1], Jason Reid[1], Uwe Dulleck[2], Ed Dawson[1]

[1] Information Security Institute,
[2] School of Economics and Finance,
Queensland University of Technology, Brisbane, Australia
{f.salim,jf.reid,uwe.dulleck,e.dawson}@qut.edu.au

Abstract. Authorised users (insiders) are behind the majority of security incidents with high financial impacts. Because authorisation is the process of controlling users' access to resources, improving authorisation techniques may mitigate the insider threat. Current approaches to authorisation suffer from the assumption that users will (can) not depart from the expected behaviour implicit in the authorisation policy. In reality however, users can and do depart from the canonical behaviour. This paper argues that the conflict of interest between insiders and authorisation mechanisms is analogous to the subset of problems formally studied in the field of game theory. It proposes a game theoretic authorisation model that can ensure users' potential misuse of a resource is explicitly considered while making an authorisation decision. The resulting authorisation model is dynamic in the sense that its access decisions vary according to the changes in explicit factors that influence the cost of misuse for both the authorisation mechanism and the insider.

1 Introduction

The three well known cornerstones of information security are confidentiality, integrity and availability. Each of these properties is defined by reference to an exogenous notion of *authorised*. For instance, confidentiality (integrity) is preserved if and only if a resource is read (modified) by an authorised user. Therefore, the complexity of preserving information security is directly dependant on *authorisation*, which is the process of mediating every requested access to resources maintained by the system and determining whether the request should be *authorised* or *denied*.

Authorisation proves to be a complex task in practice. It is based on a prediction of the users who may require access to resources to perform a job, while the correctness of this prediction appears to be inherently dependant on the future behaviour of the user. Despite this, all existing authorisation approaches inherently attempt to predict both the system's future needs (i.e., to determine who needs access) and the future user behaviour (i.e., in terms of the satisfaction of the need). To make the problem tractable, so far these two concepts have been conflated into a single construct. For example, in Multilevel Security (MLS) users are assigned clearances, or in Role Based Access Control (RBAC) to roles. Inherent in both of these assignments is the concept of 'need' and to some extent 'user's behaviour' (i.e., if users were assumed to misuse their access, they wouldn't be assigned to the role or been given the clearance). Authorisation decisions within these approaches are based on a *security policy*, that constitutes a set of rules binding access rights to users on the basis of need and assumed unlikelihood of misuse. The main shortcoming of the current policy-based approaches is their use of static criteria to determine a dynamic phenomena: future needs and future users' behaviour[3].

The adverse implication of this is significant as is discussed below under two streams of criticism, one arguing for more flexible authorisation models, another for an optimal access rights assignment. First, there is evidence suggesting that static policy may not be effective in today's dynamic environment [12,14]. As a result, a user's legitimate access request to perform a job that is beneficial for the organisation will be rejected. To address some of the rigidity of such authorisation models, risk-based approaches have been proposed [12,4,14], where an unauthorised user may be given access to resources when the risk of doing so is estimated to be below a predefined threshold. Second, there are industry surveys suggesting that a significant portion of security incidents are due to authorised users (insiders) [6]. There are several proposals to detect and prevent insider misuse by inferring user's intention through behavioural indicators captured using intrusion detection or computer forensic techniques [15,13,3].

Our research is motivated by the gap between these two perspectives: one identifies the need for more flexible authorisation models to facilitate resource sharing in dynamic environments. The other suggests, even with the current pessimistic rights assignment, misuse remains commonplace. At the heart of both lies the uncertainty about future behaviour of users. Such uncertainty is traditionally buried under an informal tradeoff analysis a priori to constructing an authorisation policy. Our goal is to make this tradeoff a dynamic decision based on explicit factors. To this end, we believe authorisation is in nature close to the principal-agent problem in the field of economics [7]. The theory has been extended to discuss the issues of delegation, especially the incentives of employers (principals) and employees (agents) to invest effort into finding the most profitable ways of using employer's resources if incentives are not, or are only partially aligned [1], a problem very similar to that of authorisation, where not to authorise a legitimate request implies that the employer has to spend additional effort to carry out the job. The implication of this perspective is profound for authorisation. It suggests that users are to be considered as self-interested; they attempt to increase their objective function without caring about the objectives of the authorisation system. Therefore, it is no longer sensible to assume users' behaviour based purely on constructs such as role, clearance or trustworthiness. For instance, a high clearance user may be more likely to misuse an access right when he is confident that it can go undetected. Whilst, a low

[3] In authorisation literature, user's compliance with policy is external to the authorisation model - assumption has been the existence of policy enforcement mechanisms.

clearance user may be less likely to misuse the same access right when she is certain about being detected and the punishment that follows.

To formally reason about potential user behaviour while making authorisation decisions we utilise techniques from game theory [5] which provide a mathematical foundation for reasoning about conflicts of interest between rational self-interested individuals. The principal contribution of this paper is the proposal of a formal game theoretic authorisation model. In this paper we deliberately introduce strong assumptions to emphasize the effectiveness of this novel approach. We introduce four types of users that an authorisation system may be interacting with, namely, benevolent, malicious, selfish and inadvertent. The type of a user defines their objective function. Further, we show that given a selfish user, under some strong assumptions, the authorisation decision is reduced to solving an inequality, representing the user's tradeoff about the misuse of a resource.

The rest of the paper is organized as follows. Section 2 discusses the related work, focusing on those employing game theoretic techniques in information security. Section 3 introduces the authorisation problem and narrows the scope of our work. Section 4 presents a game theoretic authorisation model and briefly discusses the implications of Nash equilibrium for such model. Section 6 enumerates the simplifying assumptions made in this paper and outlines possible directions for future work. Finally, Section 7 provides the concluding remarks.

2 Related Work

The marriage between economics and information security has attracted considerable attention recently. Game theory provides a mathematical framework for studying the behaviour of rational agents in a multi-player decision problem where players with different objectives can compete and interact with each other on the same system to increase their objective function. The use of game theory in modelling the interaction between users within a system has appeared in several areas of information security research, though not explicitly in addressing the authorisation problem.

Liu et al., in [10] suggest that the concept of incentives can be employed to express attackers' intentions, while the concept of utilities may be used to integrate incentives and costs in such a way that the system as well as attackers' objectives can be practically modelled. They introduce a conceptual model for determining attacker intent, objectives and strategies rather than using a specific type of game for modelling attacks; further they introduce conditions under which a specific type of game model will be feasible and desirable. Alpcan and Basar in [2] have also investigated a security game as a two player, non-cooperative, non-zero-sum game. Their work is related to ours as the game is assumed to be a complete information game and the player's optimal strategy depends only on the payoff function of the opponent. Lye et al., [16] has shown how the network security problem can be modelled as a general-sum stochastic game between attacker and the administrator. They also showed how to compute

Nash equilibria, however, their approach is specific to network security applications and they assume the benefit of attackers arises from harming the network, hence only dealing with malicious users. In [11] the authors introduce some of the problems in performing tradeoff analysis in network security. They formulate both static and dynamic Bayesian games to demonstrate the suitability of game theory for the development of various control algorithms in intrusion detection. Further, they discuss the existence of Nash equilibria for these games. However, like [16], they only deal with potentially malicious users, who may only have a positive payoff through attacking the system.

In [9], Liu et al. introduce stochastic game theoretic model for the analysis of the behaviour of malicious insiders. They suggest such a game to be a zero-sum game, where the loss of the employer is the gain of the insider. However, the zero-sum assumption is restrictive as most security games are non-zero sum [11]. Further, their model only deals with malicious insiders. It ignores the circumstances where an insider may also benefit from not attacking, which is the case for selfish insiders as will be discussed in this paper.

In another work, Liu et al., [8] propose a risk-based approach to deal with inadvertent insiders, those users who do not deliberately intend to harm the system. They propose assigning a risk budget to tasks and rewarding those employees who perform their tasks while consuming less than the allocated budget. The reward value is equal to the remaining risk tokens for the task. On the other hand, those employees who consume all their risk budget before completing their job are punished. In this way, the risk is communicated to the inadvertent insiders and the cost of risky actions is shifted from the organisation to them. However, the proposed approach is not abstract and falls short of a formal model. Further, they assume the punishment of the users is a certainty, when in reality punishment is a function of the ability to both detect an attack and administer punishment, neither of which is certain. They also assume the benefit to the user from misusing a resource is less than the punishment cost which implies the punishment is assumed to always be an effective deterrent.

The focus of our work is specifically on authorisation, where the users are not necessarily adversaries. This makes our problem distinct from the above works, because users' benefit is not always driven from attacking, as the organisation may reward actions that advance its objectives. Further, sometimes the expected cost of denying access exceeds the expected cost of authorising the access. This is contrary to the underlying belief behind existing authorisation approaches where the cost of denying access is not accounted for within the model. To the best of our knowledge, all the existing approaches to authorisation make implicit assumptions about how users will behave rather than explicitly reasoning about the users' use/misuse of resources.

3 Authorisation Problem

Let I, A, R, P respectively denote a set of all *Individuals*, *Actions*, *Resources* and *Purposes* in a system. We say $\mathbb{U} = I \times A \times R \times P$ is a set of all the possible *uses* - all the actions that can be performed by individuals on resources for any purpose. Given this, the authorisation problem revolves around the design of an authorisation function that determines a subset of uses, $\mathbb{A}^+ = \{(i, a, r, p)\} \subseteq \mathbb{U}$, referred to as the *authorised space.*

The aim of the authorisation function is to reduce the probability of an *attack*, that is defined as a user's action on a resource for a purpose other than for which the user was authorised. Formally, a usage (i, a, r, p') is an attack by user i if $\forall a, r, p \in \mathbb{U}, \exists (i, a, r, p) \in \mathbb{A}^+ \wedge \nexists (i, a, r, p') \in \mathbb{A}^+$. By definition our authorisation problem is focusing on the scenarios where resources provided to users may be used for purposes other than those intended by the authorisation system. For instance, Alice using her access permission to copy sensitive records for the purpose of financial benefit (by selling them) is considered as an attack.

An attack inherently suggests an unwelcome usage by the user regardless of the potential damage they may incur to the system. From this, we define a *user threat* (threat for short) as a probability $\rho \in [0, 1]$ of attack by a user. This expresses the unpredictability of the users' actual purpose of using the resource.

3.1 Insider Types

One of the major complexities involved in dealing with users' attacks is the fact that such attacks may be *intentional* as well as *accidental.* The former may occur for reasons such as revenge, financial gain, policy workarounds, and the latter may be an honest mistake or due to a user's lack of knowledge about the risk of their actions for the organisation [13]. Even though knowledge about intentions provides an important criteria for detecting and preventing attacks, teasing out intentions is a challenging task as there are no uniquely identifying indicators associated with attack actions [10]. Despite this, there are already several tools and approaches for detecting attacks as well as predicting them based on behavioural patterns and sequences of actions executed by a user. Although such tools are still in their infancy, the empirical results show several signs of improvement. For instance, Bishop et al., in [3] introduced an architecture for a tool that attempts to identify certain behavioural changes that may be alarming. Others [15] have suggested the use of Intrusion Detection Systems (IDS) to identify the deviations from "normal" usage patterns by users.

Here we assume such a tool exists as a function $\mathit{\Gamma}_{\{\mathit{\Theta}\}} \in [0, 1]$ that provides a probability of user's *type*, given a *type space* $\mathit{\Theta} = \{\mathit{benevolent}, \mathit{selfish}, \mathit{malicious}, \mathit{inadvertent}\}$. For example, $\mathit{\Gamma}_{\mathit{\Theta}} = \{0, 0.5, 0.5, 0\}$ suggests that that a given user might be either selfish or malicious with the probability of 1/2. A user's type embodies their *private information* that is relevant to both the user and the authorisation mechanism - each user type specifies what the user considers a utility, hence their intention:

Malicious: those who consider the loss (increased cost) of the organisation as their gain. They would like to incur as much cost to the organisation as possible. Most of the existing works deal with detecting and preventing malicious insiders [9].

Selfish: those whose aim is to maximise their own (financial) payoff. Their aim is not to incur cost to the organisation, even though this may happen as a result of their selfish choices. Hence, this type will respond to appropriate incentives (e.g., financial).

Benevolent: those who consider the loss of the organisation their loss (their utility function is the organisation's utility function), hence they do not attack.

Inadvertent: those with incomplete or incorrect information about the outcome of their actions. They are not misusing the resources (attack) to harm the organisation or doing so to increase their financial gain, but they may be careless or negligent or uninformed [8].

While our ultimate goal is to design a general authorisation model that can make an optimum authorisation decision (i.e., to reduce threat) under uncertainty about user's type, here for simplicity we will assume that for a given user the sum of her/his type probabilities is 1 and that users are only selfish ($\mathit{\Gamma}_{\Theta} = \{0, 1, 0, 0\}$). This focuses our attention on how to design an authorisation mechanism that explicitly takes into account (selfish) user's potential misuses of their access rights before making authorisation decisions.

4 Game Theoretic Authorisation Mechanism

In this section we formulate an authorisation mechanism as a game between a *selfish employee* (i) and the *benevolent employer* (j) who is the sole authority in making authorisation decisions. The game starts with a request from the employee for access to a resource. Along with the request, the employee indicates the outcome of such action for the employer, denoted as *proposal* (p)[4]. Given this request, the employer shall decide whether to *authorise* or *deny* the access to the resource[5]. On the other hand, the strategy space of the employee consists of either *attack* or *not attack*.

Such a binary description of employees' alternatives simplifies our model, however, it is no longer possible to differentiate attacks based on their consequences. For instance, given a sensitive record and a disgruntled employee with two alternative attack actions, i.e., *destroy* or *sell* the record to competitors, there may be a great difference between the two attacks from the employer's perspective, particularly if a backup of the record exists (i.e., selling it may incur a great financial loss while destroying it may merely interrupt a service).

The authorisation game centres around a resource valuable to both players. An employee may use the resource to either make a personal profit (i.e., attack) or perform a job that actions the proposal (p) for the employer. The employer,

[4] We deliberately reuse p that represented a purpose in Section 3 to draw the connection between the notion of proposal and purpose.

[5] The employer is actually the representation of our authorisation function, that given an access request $(i, a, r, p) \in \mathbb{U}$ decides whether $(i, a, r, p) \in \mathbb{A}^+$ (*authorise*) or $(i, a, r, p) \notin \mathbb{A}^+$ (*deny*) the request.

hence, is concerned about the expected cost of the attack, which causes the resource to transition from a *secure* state to a *compromised* state. Such a transition is associated with a specific monetary *cost* for the employer, denoted by C_j^r. Depending on the resource the cost of being compromised changes. In reality there may be several compromised states including loss of confidentiality, integrity, availability, privacy or reputation. Further, as we have mentioned, there may be several attacks based on the employee's action space and each may incur a specific cost depending on the causal relationship between an attack action and resource transition to a costly state. However, since *attack* generalises any single/sequence of undesirable employee actions, we assume an employee's attack incurs a cost (C_j^r) to the employer.

The employer is also susceptible to *opportunity cost*: the benefit forgone by denying a request. The quantification of opportunity is determined by the proposal (p) made by the employee to access the resource. Through such a formulation, distinct from the existing authorisation approaches, denying an access request as well as authorising it may incur a cost for the authorisation system.

Now we turn to the employee's cost factors. An employee may incur cost through *fines*, denoted by C_i^f (i.e., given they attack). However, usually a fine is not certain - it is only applicable if the employer can *detect* the attack, which is a function of the accuracy of detection techniques and the ability to *enforce* the fine. For now the ability to detect and enforce the fine is combined and referred to as the probability of being fined, denoted by $\psi \in [0, 1]$, which is assumed to be common knowledge. For example, when an employee is out-sourced from another country there may be less chance of enforcement of the fine in comparison to a circumstance when the employee is local[6]. In addition, in order to attack, the employee is assumed to incur a *preparation* cost, denoted by C_i^t. This cost abstracts the effort the employee must expend in order to acquire access to the resource to use it for personal benefit. For instance, if the resource is commercially valuable, finding a buyer requires time and effort. In other cases, the employee may need to prove to the employer that the proposal amount is attainable by him and this could require training courses and faking trustworthiness.

Sometimes the employee is given a personal benefit for the opportunity they realise. This is represented as a rate of return, $\epsilon \in [0, 1]$ on the proposed opportunity, p. We regard the predictions of the employee in terms of the actual achievement of p to be always correct if the access is granted. On the other hand, the actual personal profit for the employee from an attack is a portion $\alpha \in [0, 1]$, of the cost of resource (C_j^r), if the access is given. Note that this may not always be the case as sometimes a very costly resource for the employer has a very low value for a selfish employee or vice versa.

Given the above game setting, the game tree of employer and employee in an authorisation game is shown in Figure 4. The authorisation problem is, given complete information of both players about the payoffs, when should the employer authorise the access?

[6] For now we are not interested in the size of this fine in proportion to the loss (cost) of the employer.

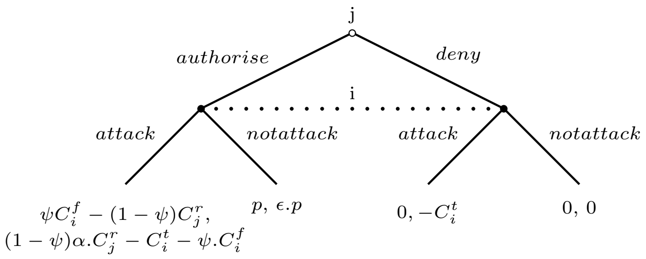

Fig. 1. Players Payoffs

4.1 Nash Equilibrium and its Implications

A solution to a non-cooperative game predicts certain strategy profiles as outcomes of the game. Defining or interpreting a solution revolves around how players reason and behave or are believed to reason and behave. This inevitably leads to the need for players to attempt to understand and predict how the other player will behave. In a game of complete information, where the strategies and payoffs are common knowledge, this is then reduced to players choosing their best responses to the potential strategy of others. The well known concept of Nash equilibrium [5] provides an exit from a cycle of speculations as to what strategies the players should use, and provides an appropriate solution for the game. In the context of the proposed authorisation game, Nash equilibrium can be defined as a set of actions from the employee and the employer such that none of them has any incentive to deviate from their chosen action.

Assuming that the employer always takes the pure strategy *deny*, then the employee's best response is *not attack*. However, this is not an equilibrium as the pure strategy of *not attack* by the employee motivates the rational employer to change his strategy to *authorise* whenever $p > 0$. By switching to *authorise*, the employee is then inclined to *attack* when

$$\epsilon.p < (1-\psi)\alpha.C_j^r - \psi.C_i^f - C_i^t. \tag{1}$$

Conversely, this can be reduced to the following: if the employer *authorises* then the employee does *not attack* if and only if

$$\epsilon.p \geq (1-\psi)\alpha.C_j^r - \psi.C_i^f - C_i^t. \tag{2}$$

The above finding is interesting and rather counter intuitive in the context of authorisation. It suggests that in making an authorisation decision the authorisation mechanism may only need to focus on the employee's payoff instead of its own. This is contrary to the existing approaches to authorisation, where there exists a policy, assumed to incorporate access rules which result from a trade-off analysis between some implicit contextual factors, for all current and future requests. Here instead, the decision factors are explicit and abstract enough to adapt to the required application. For example, the value of ψ can depend on the existing monitoring techniques, audit, accuracy of forensic techniques, physical security employed, etc.

On the other hand, the application of such an authorisation model can introduce a prescriptive system rather than simply providing authorise/deny responses. Through such an interpretation, given an authorisation request, a game theoretic authorisation model may also attempt to meet the above inequality, if not already met, through taking either or a combination of *deterrence* or *appeasement* policies. The former is to increase the cost of attacking for the user, so that the above inequality is met. This may be achieved through either increasing any or combination of ψ, C_i^t, C_i^f, or reducing α. On the other hand the appeasement policy attempts to increase the benefit for not attacking, by aligning users' utility function with the organisation through increasing ϵ. A thorough investigation of how such policies can be implemented is left for future work.

5 Case based Analysis of Authorisation Mechanism

In this section we will introduce two authorisation cases and compare a decision made under a traditional authorisation model (e.g., RBAC) to the potential decision from a game theoretic authorisation mechanism.

5.1 Case 1: Less Valuable Resource

Consider a hypothetical organisation with a role-based access control framework in place and an employee who requests to use a resource (e.g., printer), to which she does not currently have access. An RBAC model simply denies the request without considering the payoffs to the employee from misusing the printer or the payoffs to the organisation when the access is authorise/denied. Let us describe how a game theoretic authorisation model analyses the potential responses, given the following inputs[7]:

$\alpha = 1$	private benefit ratio of a resource value
$C_j^r = 1$	the cost of printing a document for organisation
$\epsilon = 0$	interest given to employee
$C_i^f = 1$	punishment cost if resource misused
$\psi = 1$	detection rate (e.g., through print logs)
$C_i^t = 0$	cost of preparation for using printer for personal purposes
$p = 1$	value of opportunity proposed (e.g., time saved)

Given the above setting the payoff for both the employee and the employer would be as shown in Figure 2. It can be seen that for the employee the rational choice regardless of the employer's action is *not attack*, and for the employer, authorising the request weakly dominates denying it, hence the pair (authorise, not attack) is the equilibrium state. This case exemplifies the authorisation dynamics for resources with a small intrinsic value, where misuses could also be easily detected.

[7] Note that the above representation of costs and punishment are ordinal numbers rather than cardinal. Hence, they show the relationship between the factors rather than their actual quantity.

		Employee	
		attack	*notattack*
Employer	*authorise*	$1, -1$	$1, 0$
	deny	$0, 0$	$0, 0$

Fig. 2. Less valuable resource and high chance of punishment

5.2 Case 2: Highly Valuable Resource

Consider a scenario where an employee of a financial firm makes stock forecasts based on some highly valuable information resources. Due to the importance of these resources, each employee only has access to a segment of the information. However, let us assume, an employee observes a good opportunity to invest in a stock, but needs some more information, which he does not have access to. Again, traditional access control models simply deny such access on the basis of their predefined policy. Let us first analyse the circumstance under the following inputs.

$\alpha =$	1	ratio of return from selling the resource
$C_j^r =$	10	the cost of selling the document to competitors
$\epsilon =$	0	employee's interest for achieving opportunity
$C_i^f =$	10	the cost of punishment
$\psi =$	.25	attack detection rate
$C_i^t =$	1	low attack preparation is needed
$p =$	3	value of opportunity proposed

Again, given the above setting the payoff for both the employee and the employer would be as shown in Figure 3.

		Employee	
		attack	*notattack*
Employer	*authorise*	$-5, 4$	$3, 0$
	deny	$0, -1$	$0, 0$

Fig. 3. Valuable resource and low chance of punishment

Given the above payoffs there is no equilibrium in pure strategies. This is because, if the employer chooses to authorise, the employee will rationally choose to attack in which case the employer switches to deny. However, when the employer chooses the pure strategy deny, then the response of the employee is not attack. Although there is no equilibrium in pure strategies, in this authorisation problem an equilibrium in mixed strategies exists: both employer and employee randomise between their pure strategies. The employer will correctly predict the employee's probabilities of possible actions, and vice versa. These probabilities make both players indifferent in choosing between their pure strategies option, thus randomizing is rational for both of them. For example, in Figure 3, if we denote by β the probability of the employer to authorise and by ρ the probability of the employee to attack, we get a mixed equilibrium for the game when $\beta = 1/5, \rho = 3/8$[8]. Given this, to prevent an attack, the authorisation mechanism authorises a request only if it believes $\rho < 3/8$.

[8] For details on mixed strategy equilibrium refer to the Chapter 1 of Fludenberg and Tirole's book [5].

In this case, the key factors behind the employee's decision to attack are the ability to monetize the valuable resource, as well as the small probability of punishment ($\psi = 0.25$), for instance because the employee is leaving the organisation. However, given the same scenario, this decision can swiftly change by the change in the probability of enforcing the punishment (C_i^f). For example, now assume that $\psi = .75$, to say the chance that the employer can enforce the punishment is high. Everything else being equal, we get the payoffs in Figure 4.

		Employee	
		attack	*notattack*
Employer	*authorise*	5, −6	3, 0
	deny	0, −1	0, 0

Fig. 4. Valuable resource and high chance of punishment

Hence, the rational action for the authorisation system in this circumstance is to authorise the access, even though the resource is sensitive and its misuse is costly. This is because the payoff of the employee reveals that attacking is not the rational choice, as the pair (3,0) is the equilibrium.

6 Future Work

In this paper we have made several simplifying assumptions to flag the potential manner of employment and benefits of game theoretic techniques in designing new authorisation mechanisms. So, our immediate efforts to improve the proposed abstract model focus on relaxing some of our assumptions: First, employer's complete information about user's type. In reality, the predication of a type involves uncertainty in the form of a probability distribution over types. Second, users alternative actions were modelled as binary, e.g., attack or not-attack. However, in reality a user may have several different attack alternatives which vary in likelihood as well as consequence. Finally, a more realistic authorisation mechanism may need to be modelled as a dynamic game rather than a one-shot static game. In dynamic games, players observe other players' behaviours and modify their strategies accordingly.

7 Conclusion

This paper discusses the authorisation problem and proposes a new paradigm of thinking for designing dynamic authorisation models. It suggests that the problem of authorisation is at it's core analogous to the principal and agent problem studied in the field of game theory. Based on this premise, it proposes the preliminary components and a basic but novel authorisation model that makes access decisions based on explicit reasoning about users available actions and the likelihood and consequences of choosing such actions, both for the authoriser and the user. Finally, it provides some extreme authorisation cases to illustrate the advantages of such a new authorisation model in comparison to the existing well-known authorisation models such as RBAC.

References

1. Philippe Aghion and Jean Tirole. Formal and real authority in organizations. *Journal of Political Economy*, 105(1):1, 1997.
2. Tansu Alpcan and Tamer Basar. A game theoretic approach to decision and analysis in network intrusion detection. In *In Proceeding of the 42nd IEEE Conference on Decision and Control (CDC)*, December 2003.
3. Matt Bishop, Carrie Gates Deb Frincke, and Frank L. Greitzer. AZALIA: an A to Z Assessment of the Likelihood of Insider Attack. 2010.
4. Pau-Chen Cheng, Pankaj Rohatgi, Claudia Keser, Paul A. Karger, Grant M. Wagner, and Angela Schuett Reninger. Fuzzy multi-level security: An experiment on quantified risk-adaptive access control. In *IEEE Symposium on Security and Privacy*, pages 222–230, 2007.
5. Drew Funderberg and Jean Tirole. *Game Theory*. MIT Press, 1992.
6. L. A. Gordon, M. P. Loep, W. Lucyshyn, and R. Richardson. CSI/FBI computer crime and security survey. Technical report, CMP Media, Manhasset, NY, 2004.
7. Bengt Holmstrom. Moral hazard and observability. *The Bell Journal of Economics*, 10(1):74–91, 1979.
8. Debin Liu, Xiaofeng Wang, and Jean L. Camp. Mitigating inadvertent insider threats with incentives. pages 1–16, 2009.
9. Debin Liu, Wanga XiaoFeng, and Jean L. Camp. Game theoretic modeling and analysis of insider threats. *International Journal of Critical Infrastructure Protection*, 1:75–80, 12 2008.
10. Peng Liu and Wanyu Zang. Incentive-based modeling and inference of attacker intent, objectives, and strategies. In *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*, pages 179–189, New York, NY, USA, 2003. ACM.
11. Yu Liu, Cristina Comaniciu, and Hong Man. A bayesian game approach for intrusion detection in wireless ad hoc networks. In *GameNets '06: Proceeding from the 2006 workshop on Game theory for communications and networks*, page 4, New York, NY, USA, 2006. ACM.
12. MITRE Corporation Jason Program Office. Horizontal integration: Broader access models for realizing information dominance. Technical Report JSR-04-132, MITRE Corporation, 2004.
13. S. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford. Insiders behaving badly: Addressing bad actors and their actions. *Information Forensics and Security, IEEE Transactions on*, 5(1):169 –179, march 2010.
14. Farzad Salim, Jason Reid, and Ed Dawson. Towards authorisation models for secure information sharing: A survey and research agenda. *The ISC International Journal of Information Security (ISeCure)*, 2010.
15. E. Eugene Schultz. A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6):526 – 531, 2002.
16. Kong wei Lye and Jeannette M. Wing. Game strategies in network security. *Int. J. Inf. Sec.*, 4(1-2):71–86, 2005.