Mapping between Classical Risk Management and Game Theoretical Approaches

Lisa Rajbhandari, Einar Snekkenes

Mapping between Classical Risk Management and Game Theoretical Approaches

Lisa Rajbhandari and Einar Arthur Snekkenes
{lisa.rajbhandari,einar.snekkenes}@hig.no

Norwegian Information Security Lab, Gjøvik University College, Norway

Abstract. In a typical classical risk assessment approach, the probabilities are usually guessed and not much guidance is provided on how to get the probabilities right. When coming up with probabilities, people are generally not well calibrated. History may not always be a very good teacher. Hence, in this paper, we explain how game theory can be integrated into classical risk management. Game theory puts emphasis on collecting representative data on how stakeholders assess the values of the outcomes of incidents rather than collecting the likelihood or probability of incident scenarios for future events that may not be stochastic. We describe how it can be mapped and utilized for risk management by relating a game theoretically inspired risk management process to ISO/IEC 27005. This shows how all the steps of classical risk management can be mapped to steps in the game theoretical model, however, some of the game theoretical steps at best have a very limited existence in ISO/IEC 27005.

Keywords: Game theory, Risk management, Equilibrium, Strategies

1 Introduction

There are many classical risk management approaches and standards [2], [19] like NIST 800-30 [17], RiskIT [7], ISO/IEC 27005 [8] and CORAS [12]. For this paper, we consider the ISO/IEC 27005 [8] standard as it provides a clear description of the stages and terminologies of the risk management process.

In a typical classical risk assessment approach, the probabilities are usually guessed and not much guidance is provided on how to get the probabilities right. When coming up with probabilities, people are generally not well calibrated. Besides, history may not always be a very good teacher. The hypothesis of the paper is: 'Gathering representative probabilities for future events that may not be stochastic, is difficult. We claim it is a lot easier to obtain representative data on how stakeholders assess the values of the outcomes of events/incidents.' In a game theoretic approach, probabilities are obtained from the actual computation and analysis. Moreover, the strategy (mitigation measure to reduce risk) can be determined with respect to the opponent's strategy. When the risks are estimated more accurately, the effectiveness of the overall risk management approach increases.

The main contribution of this paper is to show that game theory can be integrated into classical risk management. For this, we provide a clear structure of both the classical risk management and game theoretical approaches. The intention is to enable the readers to have a better understanding of both methods. We then describe how it can be mapped by relating a game theoretically inspired risk management process to ISO/IEC 27005. This shows how all the steps of ISO/IEC 27005 can be mapped to the steps in the game theoretical model; although some of the game theoretical steps at best have a very limited existence in ISO/IEC 27005.

The remainder of this paper is structured as follows. In Sect. 2, we present the state of the art and a summary of contributions. In Sect. 3, we first compare the top level perspectives of classical risk management and game theory. We then provide a more detailed mapping between the two approaches, identifying issues where a correspondence is missing. In Sect. 4, we discuss our findings. Conclusion and future work are given in Sect. 5.

2 State of the Art

The classical risk management approaches takes the perspective of the single player (individual, system, etc.) for which the risk analysis is being carried out. For example, in Probabilistic Risk Analysis (PRA), people and their actions and reactions are not given much importance [6]. Thus, Hausken [6] puts forward the way of merging PRA and game theory taking into account that, in risk assessment, the actions of the people affect each other. In addition, most of the classical risk assessment approaches are inclined to be rather subjective as the value of the probabilities of threats are either assumed or based on historical data. Taleb [18] has provided examples of Black Swan incidents that cannot be predicted accurately based on historical data.

In game theory, the incentives of the players are taken into consideration which is important in understanding the underlying motives for their actions. Liu and Zang [11] put forward the incentive-based modeling approach in order to understand attacker intent, objectives and strategies. Anderson and Moore [1] also state the importance of incentives, as misaligned or bad incentives usually cause security failure.

Game theory helps to explore the behavior of real-world adversaries [14]. Cox has stated that, by using game theory, the adversarial risk analysis can be improved [5] as the actions of the attacker, which were regarded as random variables and judged from the defender's perspective, can be computed. QuERIES, a quantitative cybersecurity risk assessment approach, uses game theory for constructing and evaluating the attack/protect model [3], [4].

While there are many papers discussing the use of game theory for specific application areas [4], [10], [16], we are aware of no works that integrate a risk management framework such as ISO/IEC 27005 and game theory.

3 Mapping between ISO/IEC 27005 and Game Theoretic Approach

In this section, we first compare the top level perspectives of classical risk management and game theory. We then provide a more detailed mapping between the two approaches, identifying issues where a correspondence is missing.

3.1 A Top Level Comparison

As stated above, there are many classical risk management approaches. To apply these approaches a clear understanding of the terminology and the overall process flow is necessary. We consider the risk management steps of the ISO/IEC 27005 [8] standard which is depicted in Fig. 1 (a). These steps can be iterated until the results are satisfactory. The input and output for each of these steps are given in ISO/IEC 27005 [8].

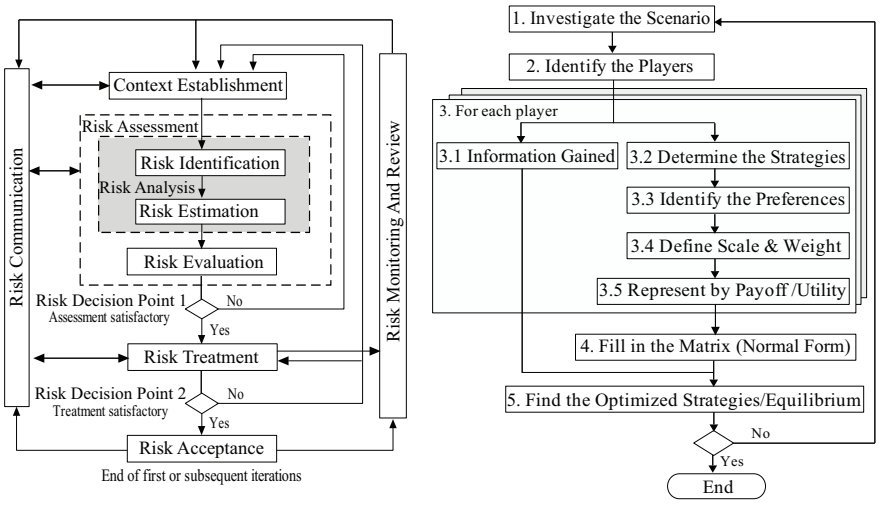

Fig. 1. (a) Information Security Risk Management Process (taken from [8]) (b) Game Theoretical Steps

Game theory helps us to understand how the strategic interactions and interdependence among the rational players influence the outcomes they gain [20], [15]. The steps that we have identified are given in Fig. 1 (b). For each of the steps, we provide a short description. In addition, Fig. 2 depicts the input and output for each of the game theoretical steps.

1. The definition of scope of interest and assets that needs to be protected are identified by investigating the scenario.

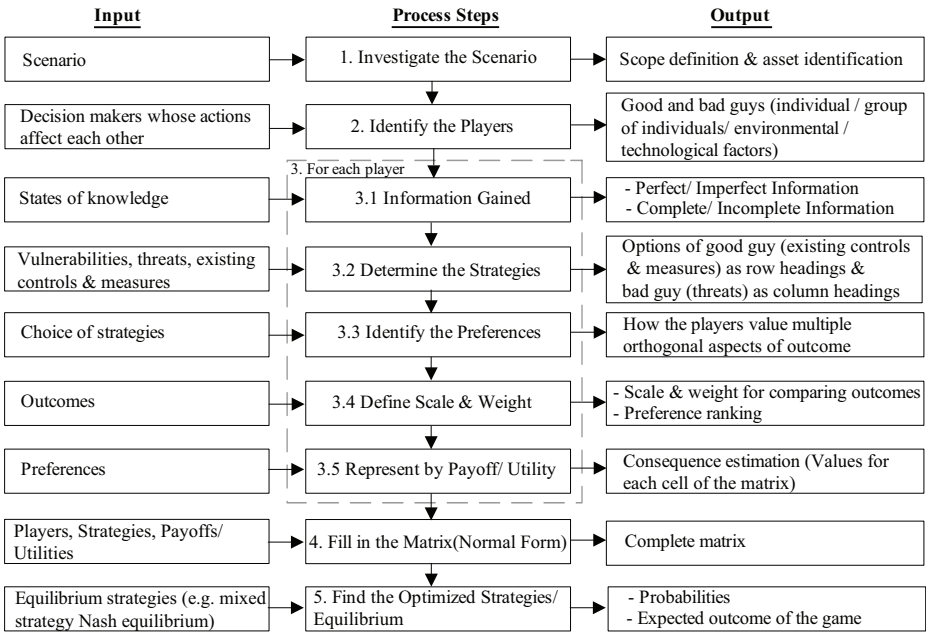

Fig. 2. Input and Output for Game Theoretical Steps

2. Players whose actions affect each other are identified. The players are inherently good or bad, and who is 'good' or 'bad' depends on the perspective of the risk analyst. If the players show seemingly irrational behavior, this can be explained by at least two alternatives: (1) given the analyst (or objective) valuation of utility, it is the players (irrational) reasoning that explains the irrational behavior; (2) the players have a different notion of utility than the risk analyst, but this notion of utility is (partially) unknown to the analyst. For the purpose of this paper, we choose the second alternative.
3. Once the players are identified, for each player we need to determine-
   3.1 Information they have when they make a decision.
   3.2 Strategies or options related to the actions of the players to overcome the threats or to gain opportunities.
   3.3 Preferences of the players, which can be obtained by asking how they value the outcomes, as the choice of each option results in an outcome. It is conceivable that players value multiple orthogonal aspects of outcome (e.g. cash, trust, reputation and legal compliance). Thus, in many cases, it may be desirable to model outcomes as vectors.
   3.4 Scale and weight should be defined so that the various outcomes can be compared. We can then rank the order of the preferences.
   3.5 These preferences can then be represented by numbers which are known as payoffs/ utilities. Higher payoffs represent more preferred outcomes. The values are assigned considering the players' motivation, capabilities

(e.g. resources to implement or defend the attack) and experiences. The players in general have the incentive to maximize their payoff.
4. The scenario can then be formulated in the normal (strategic) form.
5. The optimum strategies for each player can be identified. The combination of optimum or best strategies chosen by the players is the equilibrium and this specifies the outcome of the game to the players [13].

The process is repeated as the players' options and their outcome valuation may change. Moreover, in the long run, the entire process should be repeated for effective risk management.

3.2 Mapping Individual Steps

Table 1 shows the result of the mapping between the risk management process of the ISO/IEC 27005 standard and the game theoretical steps. For each of the process of the ISO/IEC 27005 standard, the corresponding game theoretical steps are stated. The comparison is solely based on what is provided (process steps and terminologies) in the ISO/IEC 27005 standard. Both approaches are iterated until the result of the assessment is satisfactory.

The mapping shows that all the steps of ISO/IEC 27005 can be mapped to game theory. On the other hand, we have identified that some of the game theoretical steps like information gained, beliefs and incentives of the opposing players and optimization of the strategies by the players are not included in ISO/IEC 27005.

4 Discussion

In classical risk management, risk is calculated as a *'combination of the likelihood of an event and its consequence'* [9]. The limitations in this approach are: (1) Probability is difficult to assess as the underlying process may not be stochastic. Even if the process is stochastic, lack of historical data makes the parameters of the distribution difficult to estimate. Moreover, it is not appropriate and rather subjective to use the historical data in some of the situations, for example in estimating the risk of a terrorist attack, war or extreme events (Black Swan events). (2) Probability also depends largely on the risk analyst's perception or expert elicitation. People are generally not well calibrated. Thus, it is subjective in most of the cases. (3) The beliefs and incentives of the opponent are not considered. These limitations might result in inappropriate choices and decisions, which can be overcome by using game theory.

The benefits of using game theory for risk management are: (1) The quality of data collected is likely to be better as no actuarial data is needed. It focuses on incentives, capabilities and experiences of the players rather than asking an expert for historically based probabilities. (2) Expert judgment on collected data can be audited as we can determine and investigate how the players assess the values of the outcomes, what information is available to them, and whether they

Table 1. Mapping between ISO/IEC 27005 and Game Theoretic Approach

ISO/IEC 27005 Process/ Terminology		**Game Theoretic Step/ Terminology**
Context establishment	Setting the basic criteria Defining the scope & boundaries Organization for information security risk management (ISRM)	Scenario investigation (scope definition & asset identification) Player identification (good & bad guys)
Risk identification	Identification of assets	Included in scenario investigation
	Identification of threats	Determine the strategies for the bad guys
	Identification of existing controls	Identify implemented controls i.e. 'do nothing' option for the good guys
	Identification of vulnerabilities	Options that can be exploited by threats. Included while determining the strategies for the bad guys.
	Identification of consequences	Identify how the players value multiple orthogonal aspects of outcomes. Identify the preferences.
Risk estimation	Assessment of consequences	Define scale & weight for comparing outcomes, & ranking preferences. Represent by payoff/ utility (assign values in each cell of the matrix).
	Assessment of incident likelihood	Computed probabilities for each of the strategies of both the players
	Level of risk estimation (list of risks with value levels assigned)	Expected outcome for each of the strategy of the bad guy is the risk for good guy & vice versa.
Risk evaluation	List of risks prioritized	Prioritize the expected outcome for both the players.
Risk treatment	Risk treatment options- risk reduction, retention, avoidance & transfer	Strategies (control measures) for the good guys; can be categorized into different options based on the computed probabilities.
	Residual risks	Expected outcome of the game
Risk acceptance	List of accepted risks based on the organization criteria	Strategies of the good guy (based on the organization criteria)
Risk Communication	Continual understanding of the organization's ISRM process & results.	Strategies of the good guy
Risk Monitoring & Review	Monitoring & review of risk factors Risk Management monitoring, reviewing & improving	Process is repeated as the players' options and their outcome valuation may change
Not Included		Information gained by the opponent
Not Included		Beliefs & incentives of the opponent
Not Included		Optimization of the strategies

are utility optimizing or not taking into account the strategies of the opponent. (3) Probabilities are obtained from the actual computation and analysis. However, some of the limitations related to this approach are the players' limited knowledge about their own outcome(s) and the outcomes of others, and strategic uncertainty.

ISO/IEC 27005 takes the perspective of the organization for which the risk assessment is being carried out and thus, the information gained, beliefs and incentives of the adversaries and optimization of the strategies by the players are not included. Game theory is compatible with classical risk management and can be integrated into ISO/IEC 27005. This integration will provide the risk analyst additional guidance on what issues to address in his analysis and how more auditable probability estimates can be obtained. This integration also shows that game theoretic framework can be used for the entire risk management process and not just for risk analysis.

5 Conclusion and Future Work

Clear structure for both the classical risk management and game theoretical approaches have been presented. The mapping shows that game theoretically inspired risk management process can be integrated into ISO/IEC 27005. With game theory, we can obtain representative data on how stakeholders assess the value of outcomes of incidents rather than collecting the probability of incident scenarios for future events that may not be stochastic. Moreover, game theory is a rigorous method for computing probability and also the risk analyst can achieve additional guidance on how more auditable probability estimates can be obtained. However, some steps of game theory are not included in the current version of ISO/IEC 27005.

For future work, the above approach will be explored with a comprehensive case study and extended to the iterative aspect of risk management. Moreover, we will investigate the feasibility of adopting our ideas in the context of ISO 31000.

Acknowledgment: The work reported in this paper is part of the PETweb II project sponsored by The Research Council of Norway under grant 193030/S10. We would also like to thank the anonymous reviewers for their valuable comments and suggestions.

References

[1] Ross Anderson and Tyler Moore. Information Security Economics - and Beyond. In *In Proceedings of the 27th annual International Crytology Conference on Advances in Cryptology CRYPTO'07*, pages 68–91. Springer- Verlag, 2007.

[2] P. L. Campbell and J. E. Stamp. *A Classification Scheme for Risk Assessment Methods.* Sandia National Laboratories, August 2004. Sandia Report.

[3] Lawrence Carin, George Cybenko, and Jeff Hughes. Quantitative Evaluation of Risk for Investment Efficient Strategies in Cybersecurity: The QuERIES Methodology. http://www.securitymetrics.org/content/attach/Metricon3.0/metricon3-cybenko20article.pdf. Approved for Public Release: AFRL/WS-07-2145, September 2007.

[4] Lawrence Carin, George Cybenko, and Jeff Hughes. Cybersecurity Strategies: The QuERIES Methodology. *Computer*, 41:20–26, 2008.

[5] L. A. Cox, Jr. Game Theory and Risk Analysis. *Risk Analysis*, 29:1062–1068, 2009.

[6] Kjell Hausken. Probabilistic Risk Analysis and Game Theory. *Risk Analysis*, 22(1), 2002.

[7] ISACA. The Risk IT Framework. http://www.isaca.org, 2009.

[8] ISO/IEC 27005. *Information technology -Security techniques -Information security risk management*. International Organization for Standardization, 1st edition, 2008.

[9] ISO/IEC Guide 73. *Risk management - Vocabulary - Guidelines for use in standards*, 2002.

[10] Jorma Jormakka and Jarmo V. E. Mölsä. Modelling Information Warfare as a Game. *Journal of Information Warfare*, 4(2):12–25, 2005.

[11] Peng Liu and Wanyu Zang. Incentive-based modeling and inference of attacker intent, objectives, and strategies. In *Proceedings of the 10th ACM conference on Computer and communications security*, CCS '03, pages 179–189, New York, NY, USA, 2003. ACM.

[12] Mass Soldal Lund and Bjørnar Solhaug and Ketil Stølen. A Guided Tour of the CORAS Method. In *Model-Driven Risk Analysis*, pages 23–43. Springer Berlin Heidelberg, 2011.

[13] Eric Rasmusen. *Games and information: An introduction to game theory*. Blackwell Publishers, 4th edition, 2006.

[14] Jr. Ronald D. Fricker. Game theory in an age of terrorism: How can statisticians contribute? *Springer, Heidelberg*, 2006.

[15] D. Ross. Game theory. http://plato.stanford.edu/archives/fall2010/entries/game-theory/, 2010. The Stanford Encyclopedia of Philosophy.

[16] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Qishi Wu. A Survey of Game Theory as Applied to Network Security. In *43rd Hawaii International Conference on System Sciences (HICSS)*, pages 1 –10, January 2010.

[17] Gary Stoneburner, Alice Goguen, and Alexis Feringa. *Risk Management Guide for Information Technology Systems*, July 2002. NIST Special Publication 800-30.

[18] Nassim N. Taleb. *The Black Swan: The Impact of the Highly Improbable*. Random House Trade Paperbacks, 2nd edition, May 2010.

[19] Anita Vorster and Les Labuschagne. A framework for comparing different information security risk analysis methodologies. In *Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, SAICSIT '05, pages 95–103. South African Institute for Computer Scientists and Information Technologists, 2005.

[20] Joel Watson. *Strategy : An Introduction to Game Theory*. W. W. Norton & Company, New York, 2nd edition, 2008.