A DECISION FRAMEWORK FOR EVALUATING INFORMATION RISK: GAME THEORY PERSPECTIVE

[1]NEERAJ THAKUR, [2]PARVEEN, [3]S. VENKATESAN, [4]TULASIDHARAN MUDILIAR

[1,2,3,4]Indian Institute of Information Technology, Allahabad
Email: thakur.kr@gmail.com, parveen.ind@gmail.com, venkat@iiita.ac.in, t.mudaliar@yahoo.com

Abstract—Most of the methods evolving from computer science, scuffle to consider the ambivalence factors in risk evaluation such as human errors and intentions. Thus to compute the magnitude of risk for evaluation of rational influences should also be taken into consideration to make a good decision. Game Theory is a practical approach to decision making in such scenarios and conditions. This gives the flexibility to quantify the value of risk and also to analyze all the actions that an attacker can take against the defender. This will help us examine the behavior of an attacker also, the impact and consequences; henceforth will improve our decision making process. In this paper, we have explained how Game Theory can be amalgamated with different fields like Mathematics, Computer Science and Sociology to evaluate information risk. We have described the game theoretical model that adopts various well known strategic games to serve at the different stages in enterprise risk evaluation depicting the entities involved in the process as players with certain action sets and associated payoffs or utilities.

Index Terms— Decision Making, Events, Game Theory, Information Risk, Risk Evaluation

I. INTRODUCTION

"In the absence of Information we jump to the worst conclusions" [Myra Kassim]. The rapid development of the internet community & wide spread use of Information and technology is making the environment around us highly vulnerable to the threats associated with them, leading to potentially harmful consequences that may cause loss or damage. Hence like other valued assets, there is a need to treat information as well as a protected asset and ensure sufficient safeguarding. Risk assessment and management is turning out to be of high priority to many organizations, and given the dynamic and ever changing state of information security and the threat environment, also the need to comply with many regulations, which is turning into a major challenge.

Information security risk evaluation could be classified into three main categories: First, the conventional risk assessment methods such as Fault Tree Analysis, Failure Modes Cause and Effect Analysis, MARKOV Structure, etc.; Secondly there exist standard frameworks and industry adopted best practices proposed by national or international bodies such as NIST 800-37 or ISACA Risk IT Framework, ISO/IEC 27005or those by professional organizations such as CRAMM, OCTAVE , FAIR,CORAS and so on; the third we could consider some recent quantitative risk assessment methods such as MGTBRAM, GTADM , HRCM, QuERIES and others. A general definition of risk would be the probability or threat of quantifiable damage, loss, liability, or any other negative occurrence that is caused by internal or external vulnerabilities.

Risk is determined by former attack history that will include the details & data collected for the analysis purpose. Most methods evolving from computer science fail to consider the subjective factors in risk evaluation such as uncertainties, human errors and intentions, and so on. Thus to predict the attacks & threats for risk evaluation subjective influences of the two communities should be taken into consideration to make a good decision. Game Theory is a practical approach to decision making for such scenarios and conditions. This gives the flexibility to quantify the value of risk and also to analyze all the actions that an attacker can take against the defender. This will help us analyze the behavior of an attacker & the impact & consequences of it also, this will improve our decision making process.

In this paper, we presented a strategic decision framework that uses game theory to evaluate the information risk. We have followed the concepts of security games & strategies to depict the evaluation & improved process of risk assessment that utilizes the concepts of games.

Following is the pattern that we have followed for the rest of the paper: Section Two, of this paper briefly describes the related work; Section Three presents the decision framework for evaluating information risk; and in the last section we end with a conclusion of the paper and with the possibility of future work is also accumulated.

II. RELATED WORK

Risk assessment has seen many different approaches and models often derived from widely used industry best practices. Information security risk assessment approaches broadly deals with approaching the system risk determination as a phase under the risk management program mainly identifying threats and vulnerabilities associated to a business information asset, describing risks, identifying existing controls,

determining the likelihood of occurrence, deriving severity of impact and formulating risk levels, which later will be addressed accordingly in the safeguarding phase. Macedo compares in his dissertation the various models on the basis of objectives, ease of implementation and supporting tools, which organizations could best adopt as per their needs.

Game theoretical models play an important role in information security as the field matures from its earlier qualitative and empirical nature, the mathematical abstraction provided by such quantitative models are of greater use in generalizing the problems and merging with the present ad-hoc mechanisms addressing the challenges.

Game theory has seen wide spread applications into fields such as network security modeling, compare the existing game theoretic solutions available for network security and provides taxonomy for classifying them. The ACM Survey presents set of selected works highlighting the use of game theory in solving different security and privacy problems in computer networks and mobile applications. Alpcan and Basar present how intrusions can be detected and analyzed in an access control system using game theory. They also proposed a generic model of distributed IDS with a network of sensors based on game-theoretic techniques. Numerous other works involving game theoretic approaches include modeling of security games to address an attack protect model involving computing of a Nash's equilibrium for mixed strategy approaches. Game theory models help in many security related decision making such as security investments computing Nash equilibrium and social optima for different classes of attacks and defenses. Other works propose incentive based modeling of security related activities within organizations addressing other fields of computing such as trust modeling and fields of sociology and human psychology as well.

The QuERIES Methodology talks about developing an attack/protect economic model and building of a map of the protection schemes, detailing on the specific measures applied to an IP asset, under the security plan. The map is considered to model the attacks, map and latest techniques or known methods building an attack graph using Partially Observable Markov Decision Process (POMDP).

The methodology also talks about the concept of performing a red team analysis against the information assets and further sharing information over the information markets from other red team or black hat analyses for estimating the parameters of the POMDP, this methodology helps produce an effective fundamental distribution depicting the time required to overcome a protection scheme as compared to other traditional approaches for evaluating strength of cyber security technologies.

A very interesting work in the implementation of game theory into classical Risk management framework, as compared in, the work shows how the classical approaches fail when it comes to information security as this discipline is basically a widely changing and dynamic and most probabilities are guessed and there exists no proper on guidance onto how to adapt these values.

Non – cooperative regression games with non – zero sum and incomplete information has been studied in as an approach to threat evaluation based on Bayesian network models.

Game theory has been talked about in modeling incentive based approaches to access control and management against insider threats compared to risk based access control, basically built on the idea that users are selfish and will try to maximize their net gain (incentives minus costs), a multi-person decision making problem, in which each players have a set of strategies and payoff functions. In terms of risk evaluation and mitigation, the users here could be devised incentives based on the actions they take, if any action that leads to prevention of risk or towards mitigation, they will be provided with positive incentives and similarly a cost associated to each action would determine their role in actions that could lead to security breaches.

III. FRAMEWORK

Oxford Dictionary defines framework as "a structure upon or into which contents can be put and further relates it to thoughts that are directed for a purpose". This paper proposes a framework that adopts a game theoretic approach towards information security risk evaluation, defining this process in terms of security games, help in identifying strategies to solve the problems or shortfalls identified

IV. IT RISK FRAMEWORK

Well known risk assessment models, applying to most kinds of risks, adopt both quantitative analyze such as expected value analysis, decision trees, sensitivity analysis and various modeling and simulation techniques or qualitative approaches such as scenario analysis, questionnaires, or practical toolkits such as IRAM and CRAMM.

Most organizations turn to standards and frameworks as solutions rather than as methods for organizing and representing their risk postures. The approach of game theory helps analysts look at risk with the perspective of strategic gaming hence helping map entities involved as players of the game, understanding their choices, sequence of actions, better understanding of the uncertainties (private information) and the payoffs for the chosen action profile or strategies.

V. MIXED STRATEGIES

Various strategies in game theory can be implemented of which we could broadly classify into pure Nash strategies and mixed Nash strategies. Pure Nash strategies talk about games involving multiple players, where no player can simply be benefited by varying his or her strategy. If every player has a strategy to play and no player can gain by simply changing his own strategy while all others play theirs, the payoffs here constitute to Nash equilibrium. On the other hand a mixed strategy Nash considers players with strategies consisting of action profiles with associated frequencies of how often a particular action will be chosen, here equilibrium is said to be when we have at least one player who is adopting a mixed strategy approach. Also, Nash proved that, "every finite game has Nash equilibrium but not all have a pure strategy Nash equilibrium" as talked in.

Considering the choice of strategies in information security risk assessment, we can map to a two player game, where in all possible attackers could be defined as a single attacker with a widely ranging set of actions and attack strategies comprising of various combinations of attacks. On the other hand, members of the organization involved in the risk management and information security management professionals could be broadly considered as defenders with various functions and control mechanisms adopted as actions sets.

VI. COALITIONAL GAME THEORY

Coalitional game theory for cooperation between user groups or within divisions of an organization towards Info sec awareness and meeting the objectives.

Cooperative games having more than one person are Coalition Games, where they do not have any constraint on the agreements between the players who have formed the alliance. Coalitional approach lets the player use a side payment that is allowed by transferrable utility. These side payments are used by players using mutually beneficial strategies to achieve the same goal. Players having same goals and targets will be able to form a group working together towards that goal is called a coalition.

Functions showing characteristics of strategic form

- Suppose $p \geq 2$ is the number of players from 1 to p , and P is the set of players, $P = \{1,2,3,...,\mathrm{p}\}$. Q defines the coalition as a subset of P , $Q \subset P$. 2^P is the set of all coalitions. This set P is the grand coalition.

Suppose there are three players $p = 3$, then the number of coalitions will be eight, $\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\mathrm{P}\}$. Hence (P,r) is the pair of a p -person coalition game, where $P = \{1,2,...\mathrm{p}\}$ is the set of players and r is a real-valued function, that is defined as a function showing characteristic of that strategic game, on the set 2^P , of all coalitions and satisfying

i) $\mathrm{r}(\varnothing) = 0$, and

ii) if $M \cap N = \varnothing$, then $\mathrm{r}(\mathrm{M}) + r(\mathrm{N}) \leq r(\mathrm{M} \cup N)$

Here the first statement explains a set having zero value or empty set, and second statement explains M and N are two disjoint coalitions that has a bigger value outcome, but they are even bigger when working together.

We implement this approach when we have two or more than two players in an organization that are working towards the same goal. This takes up the approach of forming an alliance after sharing certain mutually beneficial strategies to achieve the close objectives. Coalition also has close relation with strategic form of a p -person game that is given by 2n-tuple, $(A_1, A_2, A_3 ....., A_n, Z_1, Z_2, Z_3 ....., Z_n)$ where

for $i = 1,...,\mathrm{p}, \mathrm{Z}_i$ is the set of player i , having pure strategies and to player i , the payoff function is $i = 1,...,\mathrm{p}$ $z_i(\mathrm{a}_1, \mathrm{a}_2, ..., \mathrm{a}_n)$ when player 1 uses $a_1 \in A_1$, player 2 uses $a_2 \in A_2$, ..., and player p uses $a_n \in A_n$.

Every finite p -person game can be reduced to coalitional form that right now is in strategic form. Reduction of such a form to coalitional game has the ability to loses important features that could be counted as a threat. The crisp implementation of this form of game that is coalition can be seen in the paper Coalitional Game Theory for Security Risk Management that explains both Non cooperative and cooperative games with ideal coalition as well.

VII. MARKOV APPROACH

Markov model, also talks about the approach of Markov chain that describes how the process of potential threats are spreading and then assess the system risk based on this chain result. A system simulating the threat that is in propagation along with the concealed risk is depicted with another Markov chain that is having the capability to portray repair process. System Administrator implements this chain and then reduces the impact of threat caused by a vulnerability thus making the system less threat prone. This Markov model follows the approach of two player game strategy that are threat agent and vulnerability agent where the risk is increased and reduced according to the decrement in threat and vulnerability by the repair process. They have two states through which the transition is taking place and that are: Threat State and Vulnerability State along with State Space and Action Space. This model has

introduced a function called Damage Function, that will keep track of the damages done by a threat to the asset at the moment x in the network system.

Based on the above principles of game theory, we suggest a logical & dynamic approach to evaluate the information risk illustrated in Fig 1. This framework briefly discusses the mathematical model of risk articulation. Especially, it emphasizes on the practical implementation of game theory and different type of games that can be played at various sub levels of an organization to effectively

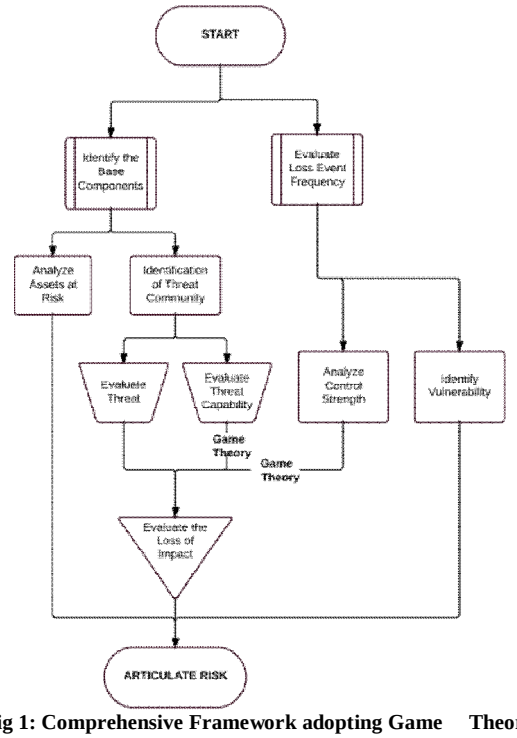


Fig 1: Comprehensive Framework adopting Game Theory

measure the information risk. It consists of three basic factors: Asset, Vulnerability, and Threat and then further in this framework we have divided these subjective terms in such a way that we have a good possibility of getting the right values of risk.

The proposed framework is built on an exhaustive and quantitative computational approach from the field of economics, computer science, games and decision theory. Adopting the idea from the QuERIES methodology the framework includes an approach to construct a game theoretic based attack protect model based on all possible threats and vulnerabilities associated to critical information assets. A probability distribution representing an attacker's multi-staged decision processes and knowledge can be mapped in terms of an attack graph. The POMDPs can help model a framework an attacker or defender would adopt towards defeating or ensuring protection of any valued information asset. Further, once the probabilities for each state and costs having estimated.

We could invite a red team or black hat team to conduct an analysis or use the concept of information markets, wherein the organization discloses to some extent its security protections to help estimate the underlying parameters and hence manage to compute optimal policies for the POMDP.

CONCLUSION

In this paper, we have given a precise description of the risk articulation process with different types of games. A literature review has been carried out to figure out what all parameters could be a fit for the risk articulation process with an overview of different methodologies used in the history of game theory. Two parameters that could be a good fit are identified as: Threat Capability and Control Strength. This paper uses the approach of attack / protect model for risk evaluation devised on the basis of game theory. We have also introduced the implementation of coalition within this supporting structure and Markov state change approach to compute probability distributions of possible attacks and computation of optimal policy for the protection scheme.

As future work, a real time scenario analysis will help check the feasibility of the approach, also, we plan to design business process models to implement within an enterprise. This process can be carried out in a simulated environment to help seek better results for computing the efficient protection schemes, under real world circumstances.

REFERENCES

[1] IEC 1025: 1990 Fault Tree Analysis (FTA), 1990

[2] Bouti, A. and AitKadi, D., "A State of the Art Review of FMEA/FMECA", International Journal of Reliability, Quality and Safety Engineering. January 1949: 515-543.

[3] B. Littlewood, "A reliability Model for Systems with Markov Structure", Applied Statistics, 1997, 24(2):172~177.

[4] Guide for Applying the Risk Management Framework to Federal Information Systems by NIST

[5] The Risk IT Framework - Information Systems Audit and Control Association, ISACA

[6] Klipper, Sebastian. "ISO/IEC 27005." Information Security Risk Management. Vieweg+ Teubner, 2011. 63-97.

[7] vonSolms, Rossouw, et al. "A framework for information security evaluation." Information & Management 26.3 (1994): 143-153.

[8] Alberts, Christopher J., and Audrey Dorofee. Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc., 2002.

[9] jones, J. An Introduction to Factor Analysis of Information Risk (FAIR) - A framework for understanding, analyzing, and measuring information risk. 1st ed. [ebook] Risk Management Insight, pp.1-76.

[10] Availableat:http://riskmanagementinsight.com/media/documents/FAIR_Introduction.pdf

[11] Vraalsen, Fredrik, et al. "The CORAS tool-supported methodology for UML-based security analysis." (2004).

[12] A Markov Game Theory-based Risk Assessment Model for Network Information System - Cui Xiaolin, Tan Xiaobin, Zhang Yong,XiHongsheng

[13] He, Wei, et al. "A game theoretical attack-defense model oriented to network security risk assessment." Computer Science and Software Engineering, 2008 International Conference on. Vol. 6. IEEE, 2008.

[14] Zhao, Dong-mei, Jian-feng Ma, and Yue-sheng Wang. "Model of fuzzy risk assessment of the information system." JOURNAL-CHINA INSTITUTE OF COMMUNICATIONS 28.4 (2007): 51.

[15] Carin, Lawrence, George Cybenko, and Jeff Hughes. "Cybersecurity strategies: The queries methodology." Computer 41.8 (2008): 20-26.

[16] Macedo, Filipe, and Miguel Mira da Silva. "Comparative Study of Information Security Risk Assessment Models."

[17] Apostal, David, et al. "Network security modeling system and method." U.S. Patent No. 7,315,801. 1 Jan. 2008.

[18] Baskerville, Richard. "Information systems security design methods: implications for information systems development." ACM Computing Surveys (CSUR) 25.4 (1993): 375-414.

[19] Alpcan, Tansu, and Tamer Basar. "A game theoretic analysis of intrusion detection in access control systems." Decision and Control, 2004. CDC. 43rd IEEE Conference on. Vol. 2. IEEE, 2004.

[20] Alpcan, Tansu, and Tamer Basar. "A game theoretic approach to decision and analysis in network intrusion detection." Decision and Control, 2003. Proceedings. 42nd IEEE Conference on. Vol. 3. IEEE, 2003.

[21] Roy, Sankardas, et al. "A survey of game theory as applied to network security." System Sciences (HICSS), 2010 43rd Hawaii International Conference on. IEEE, 2010.

[22] Liu, Peng, WanyuZang, and Meng Yu. "Incentive-based modeling and inference of attacker intent, objectives, and strategies." ACM Transactions on Information and System Security (TISSEC) 8.1 (2005): 78-118.

[23] Bulgurcu, Burcu, Hasan Cavusoglu, and IzakBenbasat. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." MIS quarterly 34.3 (2010).

[24] Carin, Lawrence, George Cybenko, and Jeff Hughes. "Cybersecurity strategies: The queries methodology." Computer 41.8 (2008): 20-26.

[25] Russell, S. J. and Norvig, P. 2002. Artificial Intelligence: A Modern Approach (2nd Edition). Prentice Hall, New York, NY

[26] Rajbhandari, Lisa, and Einar Arthur Snekkenes. "Mapping between classical risk management and game theoretical approaches." Communications and Multimedia Security. Springer Berlin Heidelberg, 2011.

[27] Johansson, Fredrik, and Goran Falkman. "A Bayesian network approach to threat evaluation withapplication to an air defense scenario." InformationFusion, 2008 11th International Conference on. IEEE, 2008.

[28] Debin Liu, Ninghui Li,XiaoFeng Wang, L. Jean Camp. "Beyond risk-based access control: towards incentive-based access control." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2012. 102-112.

[29] Wang, Weihong, and Baochun Li. "To play or to control: a game-based control-theoretic approach to peer-to-peer incentive engineering." Quality ofService—IWQoS 2003. Springer Berlin Heidelberg, 2003. 174-192.

[30] Maillé, Patrick, Peter Reichl, and Bruno Tuffin. "Of threats and costs: A game-theoretic approach to security risk management." Performance Models and Risk Management in Communications Systems. Springer New York, 2011. 33-53.

[31] Ferguson, T. (n.d.). Game Theory. 1st ed. [ebook] University of California at Los Angeles, pp.3-27. Available at: http://www.math.ucla.edu/~tom/Game_Theory/coal.pdf

[32] Saad, Walid, TansuAlpcan, Tamer Basar, and A. Hjorungnes."Coalitional game theory for security risk management." Internet Monitoring and Protection (ICIMP), 2010 Fifth International Conference on. IEEE, 2010.

[33] Dan Shen et al., "Adaptive Markov Game Theoretic Data Fusion Approach for Cyber Network Defense", IEEE Conference on MilitaryCommunications, October 2007.

★★★