IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 3 Issue 1, January 2016.
www.ijiset.com
ISSN 2348 – 7968

Cyber Security using Game theory

Dipak V Bhosale[1], Prajakta K Mitkal[2] and Yogesh S Lonkar[3]

[1,2,3] Computer Science and Engineering, Karmayogi Engineering College, Shelve, Pandharpur, Maharashtra, India

Abstract

Cyber Security is a complex concept that depends on the domain knowledge and requires cognitive abilities to determine possible threats from large amount of network data. Strengthening the security and resilience of cyberspace has become an important homeland security mission. Game theory is famous theory for detecting the threats as well as preventing the threats. In analysis various attack strategies can be considered such as inflation, deflation and Oscillation. Game theory provides the basic training and awareness of key algorithmic principles and lessons learned. In Game theory, the defense strategies are outlier detection and Adaptive Threshold selection. Using game theory the user can easily detect the intruders and provide the solution for the problems in step by step manner, which is easy and understandable language.

Keywords: *CyberNEXS, Game theory, Cyber Security, Network Security, Game Design*

1. Introduction

1.1 The Cyber Security

Computer security, which can also be known as cyber security or IT security is the protection of information systems from thefts or damage to the hardware, software and to the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as software access that come via network, due to malpractice of operators, which can be either intentionally or accidentally or being tricked into deviating secure procedures.

Computer security covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction and the process of applying security measures to ensure confidentiality, integrity and availability of data. There are various vulnerabilities and attacks such as Backdoors, Denial of service attack, direct access attacks, Eavesdrop, etc. On considering the scenario of daily committed crimes, the security of the computer systems has become imperative to minimize and possibly avoid the impact of cybercrimes [1]. Various system such as Intrusion Detection System can be helpful, which can examine how an individual detect malicious events and declare an attack based on a sequence of network events and for operating this system there is no requirement of having knowledge of cyber security [2].

1.2 Game theory

Game theory describes scenario by considering it as game which consist of players, where each player chooses actions which result in the best possible rewards for self, while anticipating the rational actions from other players [3]. Game theory provides powerful tools that allow us to model an advanced adversary who knows how and what defense strategies are used and can adjust his attack strategies accordingly [4].

CyberNEXS gaming is considered as de facto standard in cyber defense competitions due to its wide cyber security training tools and certification of professional cyber security [5].

2. Literature Survey

2.1 A Review of the advances in Cyber Security benchmark datasets for evaluating data driven based intrusion detection systems, 2015.

This paper deals with the scenario, cybercrimes, which leads to heavy loss. It also gives the reviews of the advance enhancement in the cyber security by considering the dataset for the evaluation of machine learning and data mining based intrusion detection system. The datasets considered are of KDD and UNM (University of New Mexico), which lost their relevance because of the significant changes in computer technology. And as solution they introduced, ADFA-LD cyber security benchmark dataset.

2.2 Effects of Cyber Security knowledge on attack detection, 2015.

A security of computer is current booming issue in each event. A security analyst needs to be situated, which

ISSN 2348 – 7968

has the domain knowledge to benefit from all available data sources and visualizations. Analyst should have theoretical as well as practical knowledge, and also must be quick to learn and adapt the novel and dynamic environments.

2.3 A survey of Game Theory as applied to Network Security.

As hackers activities are significantly increasing, there is need of developing an infrastructure which can not only detect the hacker threat but also prevent it. Game theory is a concept which help user to detect the hacker threats as well as provides the solution for that treats. In addition it also provides the awareness to society people using the game playing concept, in step by step levels.

2.4 Applying Game Theory to analyze attacks and defenses in virtual coordinate systems.

As Game theory is used for detecting and analyzing the threats over the network. In this paper, Virtual Coordinate system is used which provides accurate and efficient services that allows user to determine latency to arbitrary users based on information provided by subset participating nodes.

2.5 Exploring Game Design for Cyber security Training, 2012.

This paper includes the main concept of Game theory, which is used for detecting and analysis of threats in network. Game theory also provides the awareness in user that is using the network in large amount. This awareness can be provided by training, which includes cyber security topics such as Password usage and management, Protection from malware and spam, Patch management, social engineering phishing techniques, etc. The main concept here used is CyberNEXS gaming, which is considered as de facto standard in cyber defense competitions due to its wide cyber security training tools and certification of professional cyber security.

3. Game Theory: Training and Awareness

Game theory is a framework which is mainly order to identify the best attack and defense strategies assuming that the attacker is aware of the defense mechanisms [4]. Game theory has its main goal to create awareness of different possible attacks, with the help of training [5]. User effective security training can enhance the assurance of the information posture of the organization [6]. There are various tools available for providing training such as video game like tool CyberCIEGE, which has targeted for the requirement of specific organization. Game theory mainly includes two type of optimization that are, Mixed initiative optimization and Multi objective optimization [7]. Most commonly used current training and awareness techniques are as follows:

3.1 Formal Training Sessions

This is personnel traditional approach which generally conducted in department of Navy, which include the training of engaging the audience for long duration [6].

3.2 Passive computer based and web based training

This is centralized approach, which includes the slide show with no dialogues on the awareness problems [6].

3.3 Strategic placement of awareness messages

This approach raise the level of consciousness through the delivery of messages in the workplace using newsletters, memos, emails, screensavers, posters, etc [6].

3.4 Interactive computer based training

This approach is carried out using video games which is categorized into two classes that are, first person interaction games or resource management simulations. The games included are like shooter games or problem solving games [5].

As it is game theory, the main focus is on Player entity and its activities on each topic of awareness, which is as follows:

Table 1 Basic awareness topics and player activities

Sr. No.	Topic	Player activity
1	Introductory IA briefing	Definition and description of IA elements and their interaction
2	Information Value	Protect high value information
3	Access control	On both mandatory and discretionary access control
4	Social Engineering	Scenario is presented to player which leads to social attack
5	Password Management	Preventing game character

ISSN 2348 – 7968

6	Malicious software and basic safe computing	Determine and expend resources to procure procedural settings that prevent from these software
7	Safeguarding data	Situation is provided where player has to take action
8	Physical security mechanisms	Selecting cost effective physical security for sensitive areas

4. Why Game theory?

Mostly the security threats are originated from inside the organization, which is also referred as Insider's threats, which leads to loss of intellectual property. According to survey 70+% security problems are from organization itself [8].

4.1 Reasons of occurrence of threats

Before going to the solution of problem, the main thing is to find how are the threat creators and why?
If we consider Insider threats then they are caused either by current or ex-employees, contractors or partners, who are authenticated to the access of organization [7].
It is also became an easy task because of easily available tools of hacking on internet, USB devices and wireless connectivity, which consist of easy break-ins.

So, to avoid these threats and to retrieve the prevention from these threats, some solution is required. To acquire solution, Game theory is one concept which is easy to understand and compatible.

4.2 Challenges

While providing prevention following are the challenges that to be known to the analyst:

a) Prevention of unauthorized system access to critical IT resources
b) Prevention of data breaches
c) Prevention from Insider attacker
d) Preventing theft of intellectual property
e) Reducing the cost of administration to security
f) Providing better audit ability to address compliance requirements.

5. Game theory

Game theory depicts the multi-person decision scenarios as games where each player is considered as an entity which chooses actions, which result in best possible reward for self [4]. Game theory consists of various terms that are:

a) Player: A basic entity of game who makes decision and then performs action.
b) Solution concept: Systematic description of how the game will be played by employing the best possible strategies.
c) Consequence function: Associates a consequence with each action the decision maker take.
d) Preference relation: Complete relation on the set of consequences which model the preference of each player in the game.
e) Strategy: Complete plan of actions in all possible situation throughout the game.
   a. Pure Strategy: If strategy specifies unique action
   b. Mixed Strategy: If plan specifies a probability distribution [5].

5.1 Classification of Games

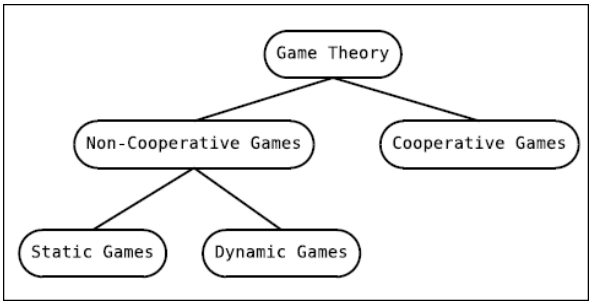

Figure 1 Classification of games

In the classification of games, the game theory is classified into Non-cooperative games and cooperative games as shown in figure 1.

Non cooperative games are further classified into Static and Dynamic games [6].

5.1.1 Static Games

A one-shot game in which plan of action is chosen by each player and decision is made simultaneously, that is while choosing the plan each player is not informed of plan of action chosen by other player.

In figure 2, each rectangular leaf node lists the research works which fall under the corresponding category and each research work is represented by the reference number and the first author name.

ISSN 2348 – 7968

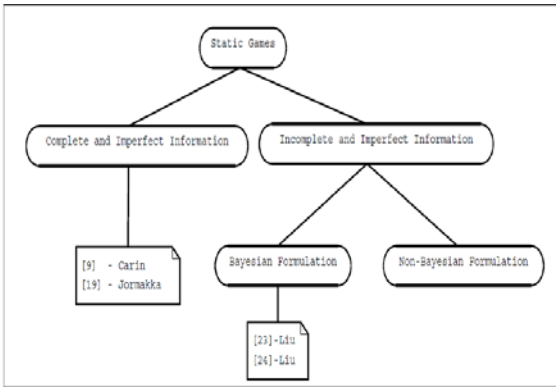

Figure 2 Static Games

Static games consist of complete imperfect information and incomplete imperfect information.

- Complete imperfect information, computational approach in which, for each scenario the authors found the best strategy of the players in a quantitative form.
- Incomplete imperfect information, an methodological approach which observes the ability to model and infer attacker intent, objective and strategy [6].

5.1.2 Dynamic Games

A game with more than one stages in each of which the players can consider their action.

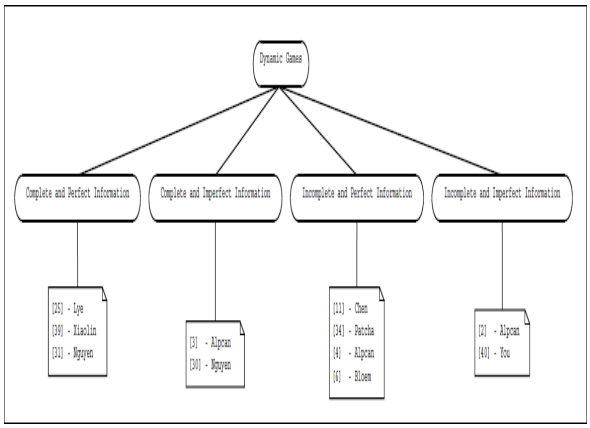

Figure 3 Dynamic Games

In figure 3, each rectangular leaf node lists the research works which fall under the corresponding category and each research work is represented by the reference number and the first author name.

Dynamic games consist of Complete perfect information, Complete and imperfect information, Incomplete and perfect information and Incomplete and imperfect information.

- Complete perfect information, an formal model in which, an enterprise network is viewed as a graph of 4 nodes that are web server, file server, work station and external world along with the traffic state for all the links.
- Complete Imperfect information, an model that has interaction between malicious attackers to a system and an Intruder Detection System using stochastic game.
- Incomplete Perfect information, used to design the response for the importance scanning Internet worm attack.
- Incomplete Imperfect information is model which has interaction of an attacker and the network administrator as a repeated game with finite steps and infinite steps [6]

.

6. Conclusion

As strengthening the security and resilience of cyber has become an important task, Game theory helps to detect the threat which helps to make strong network since it also has the prevention training. Game theory training can be facilitated to user, so that awareness can be built in user mind.

References

[1] AdamuAbubakar, HarunaChiroma, SanahMuaz, LibabatuBaballeIla, “A Review of the advances in Cyber Security benchmark datasets for evaluating data driven based intrusion detection systems”, Elsevier, Science Direct, SCSE 2015.

[2] Noam Ben-Asher, Cleotilde Gonzalez, “Effects of Cyber Security knowledge on attack detection”, Elsevier, Sciencedirect, Computer in Human behavior journal, Feb, 2015.

[3] Sankardas Roy, Charles Ellis, Sajjan Shiva, DipankarDasgupta, VivekShandilya, QishiWu, “A survey of Game Theory as applied to Network Security” ONR, N00014-09-1-0752.

[4] Sheila Becker, Jeff Seibert, David Zage, Cristina Nita Rotaru, Radu State, “Applying Game Theory to analyze attacks and defenses in virtual coordinate systems”.

[5] Ajay Nagarjan, Jan Allbeck, ArunSood, “Exploring Game Design for Cybersecurity Training”, IEEE international conference, 2012.

ISSN 2348 – 7968

[6] Benjamin D Cone, Michael Thompson, Cynthia Irvin, thuy Nguyen, “Cyber Security Training and Awareness through Game Play”, IFIP, Volume 201, 2006.

[7] MilindTambe, Manish Jain, James Adam Pita, Albert Xin Jiang, “Game Theory for Security: Key Algorithmic principles, Deployed systems, Lessons learned”.

[8] SugataSanyal, AjitShelat, Amit Gupta, “New Frontiers of Network Security: The threat Within”.