Researching the Applicability of Mathematical Approaches for Modeling Cyber Security Processes

Anastasiia Strielkina and Dmytro Uzun

National Aerospace University "KhAI", Kharkiv, Ukraine
{a.strielkina, d.uzun}@csn.khai.edu

Abstract. As the title implies the article substantiates the applicability of mathematical approaches for modeling cyber security processes. The article gives a detailed analysis of applicability of Markov processes and Game theory approach. In addition, the authors give requirements that can be applied for developing models . The authors come to the conclusion that it is necessary to use several mathematical approaches to describe a more complete model of information system cyber security processes.

Keywords: Cyber Security, Mathematical Models, Modeling, Game Theory, Markov process.
Key Terms: MathematicalModel, Model, Process, Research.

1 Introduction

In most cases during designing of complex systems resort to a modeling of main processes, occurring within the system and at the junction of environment and system. Furthermore, models can be used for monitoring and security auditing on the stages of exploitation and maintenance of information system [1-3].

Today, the relevance of the problem of cyber security does not raise any doubts. Unfortunately, this problem is far from being absolutely solved. The main limitation of the current cyber security state is that the security approach is largely heuristic, increasingly burdensome, and it is struggling to contend with expeditiously evolving threats and risks.

In this paper, modeling refers a mathematical modeling allowing to obtain a formal description of the information system and further to make a quantitative and qualitative evaluation of its performance. Based on the analysis of existing scientific publications it is possible to identify such theories to model the processes of cyber security:

- The probability theory;
- The stochastic processes theory (Markov processes, semi-Markov processes, branching processes);
- The Petri nets theory;
- The theory of automata;

- The graph theory;
- The theory of fuzzy sets;
- The game theory;
- The theory of catastrophes, etc.

The differences of most models are which parameters they are using as input and which as output after the settlement. Typically as input data is used the collected statistics on existing information systems or data experts.

Furthermore, modeling methods based on informal systems theory: structuring techniques, estimation methods and methods for finding optimal decisions become widespread. The combination of methods of these three groups allows expanding the possibility of applying formal theories to conduct a full-fledged simulation of protection systems.

The aim of this work is substantiation of the correctness of using Markov processes and Game theory for modeling cyber security processes.

2 Related Works

This section briefly discusses the existing body of other research related to the survey topic of this paper.

Authors of [4] demonstrated the mathematical approach to predict and detect intrusion in the network.

Abraham and Nair [5] provided limited insight into understanding the impact of attacks have on the overall security goals of the network and the system.

Authors of [6] have been exploring the applicability of game theoretic approaches to address the network security issues. That paper surveys the existing game-theoretic solutions, which are designed to enhance security, and presents a taxonomy for classifying the proposed solutions.

Chung et al. [7] show that attacks are highly dependent on human-driven decision-making. Authors found the limitation on applying such method on security games.

Above-mentioned and other existing works do not justify the choice of models, do not show cyber security requirements to models or just give theoretical frameworks for constructing of models.

3 Mathematical Approaches

3.1 Applicable Criteria to Models

According to the analysis of existing research papers and taking into account practical considerations, requirements for the model of cyber security processes are distinguished abilities to calculate:

- A probability of threat;
- An implementation time of threat;

- A vulnerability detection time;
- The damage (and loses) after successful attack;
- The cyber security risks, etc.

All the above-listed requirements should depend on used protection means, techniques, tools, vulnerabilities in them and the level of experience and equipment of the intruder.

As probabilities can be used expert assessments, statistical data from open sources.

3.2 Markov Processes

A successful attack on an information system with significant reservations can be interpreted as a rejection of the reliability theory. In the reliability theory for modeling of systems with refusals and restoration of the objects is typically used Markov processes.

Highlighting the stochastic parameters of the threat vulnerability, namely, an intensity of appearance (detection) λ and an intensity of elimination μ, it is possible to describe an appropriate mathematical model which is able to determine necessary probabilities of information system cyber security processes $P_0=f(\lambda, \mu)$.

In general, an enlarged graph of Markov model of cyber security process in information system as a whole, which is established by N threats of attacks, is shown in Fig. 1. The intensity of transition to the absorb state S_n can be determined as the intensity of a real threat of attacks λ_{tn} and an availability rate of an intruder to the attack K_{an}, $n=1,\ldots, N$.

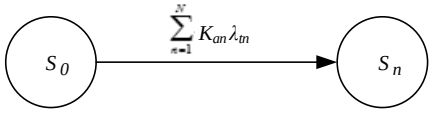

Fig. 1. Enlarged graph of the system

Practical use of the enlarged model will simplify the modeling, reducing it to simple tasks. Markov model allows calculating the probability of a successful attack, identifying the most dangerous threats.

3.3 Game Theory

Game theory is a mathematical theory of conflict situations. The primary elements of the Game theory are:

- Game (a simplified mathematical model of conflict);
- Players (a multiplicity of stakeholders);
- Action (choice of options envisaged by the game rules);
- Rules (conditions which determine the options of the players' actions);
- Strategy (possible actions of each of the parties);

- Payoff (gain or loss of each player, which may be expressed in money or material values).

According to [6], games can be classified as shown in Fig. 2. On this basis, games are classified into non-cooperative and cooperative. In its turn, non-cooperative games are divided into static and dynamic. Detailed reviews of each type of games are already represented in many works [8-13] in the framework of cyber security research.

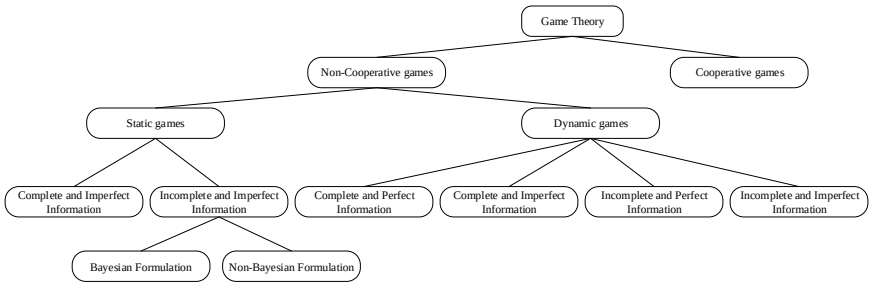

Fig. 2. Classification of games

To describe the model based on Game theory approach it is necessary to have such input parameters and actions:

- An availability of threats classification;
- Carrying out risk analysis, which shows an expected amount of losses in the case of successful attack;
- Formal description of protection means (the probability coefficient, which shows how decreases the probability of a successful attack on the system and the cost of the technical facilities and measures for bringing information systems in line with the requirements).

In general, the two sides of the game can be defined as a set:

$$G=\{x,y,W(x,y)\}, \quad (1)$$

where W – payoff of the game;
x – strategy of player 1;
y – strategy of player 2.

The most optimal and interesting strategy for consideration is the mixed strategy with a finite number of states. These strategies consist of the use of several pure strategies, alternating randomly. In this case, the gain will be equal to the payoff of the game.

Constructed the payoff matrix and it's analyzing can assess in advance the consequences of each decision, obviously, reject failed options to ensure security solution and recommend the most effective options for the entire range of attacks, given x_i strategies. If the payoff matrix is constructed in which the game results w_{ij} are losses due to the successful attack, the best in terms of available information on the nature of

will be the strategy, in which the average loss will be minimal, that is, the minimum amount:

$$\sum_{i=1}^{n} w_{ij} \cdot p(x_i) \rightarrow min\ . \tag{2}$$

Game models are used to solve the problem of the choice of solutions providing optimal parity between the cost of protection and reduced risk of system exploitation.

Models constructed on the basis of Game theory does not take into account strategies of attacker's behavior depending on its readiness and equipment, also not taken into account the possibility of threats and therefore damage in various ways.

4 Binding of the Models

The analysis of approaches to modeling information system cyber security processes has shown that none of the models meet the full the basic established criteria.

Markov process uses abstract states of processes, making it difficult to use the models to real systems. Models constructed on the basis of Game theory does not take into account strategies of attacker's behavior depending on its readiness and equipment, also not taken into account the possibility of threats and therefore dam-age in various ways.

For a more detailed modeling of cyber security processes, we propose to use an approach, which uses some mathematical models (in this paper Markov processes and Game theory approach) as shown in Fig. 3.

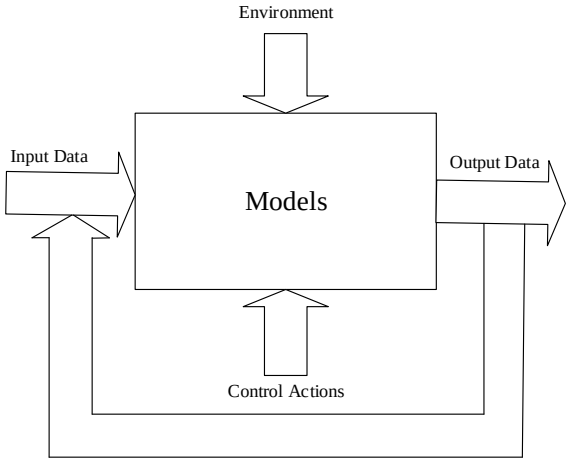

Fig. 3. The general model of cyber security models

According to this, input parameters for this model are parameters for each model (as considered above):

- The classification of threats (also possible of vulnerabilities);
- The classification of protection tools/ techniques;
- The expected amount of losses (damage);
- The probabilities of the implementation of different types of attacks;
- The probabilities of the detection of different types of attacks;
- The probabilities of the countering of different types of attacks, etc.

Initially, it is the collected statistics on existing information systems or data of experts, and then input parameters on the *t+1* step will depend on output parameters on *t* step. Output parameters are applicable criteria to models as discussed above (e.g., the probabilities of threats, the implementation time of threat, the vulnerability detection time, the damage (losses) after the successful attack, cyber security risks, etc.). In addition, developed model should depend on environment and control actions.

Related works contain only general guidelines for building the binding model, but do not give any practical applications. In this paper, an attempt was made to combine models by providing a functional linkage in the form of a feedback scheme. The general model is proposed only without detail definition of assembly Markov processes and Game theory models (like "black box" represented as the input data and the first steps of construction). The proposed model is based on the assumption of the possibility of the taking of each model and a feedback mechanism is provided for the possibility of control and management.

5 Conclusion and future work

To the main results of the work can be attributed substantiation of the correctness of using Markov processes and Game theory for modeling cyber security processes. It is shown that a single model cannot solve all requirements to the cyber security system. Therefore, it is necessary to use several mathematical approaches to describe a more complete model of information system cyber security processes.

Our future work includes investigation of other mathematical approaches, development of models, statistics gathering and simulation of models.

References

1. International Organization for Standardization: ISO/IEC 15408:2009, Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and general model (2009).
2. International Organization for Standardization: ISO/IEC 27000:2016, Information technology – Security techniques – Information security management systems – Overview and vocabulary (2016).
3. National Institute of Standards and Technology: The NIST Cybersecurity Framework (2014).
4. Brindasri, S., Saravanan, K.: Evaluation of network intrusion detection using Markov chain. In: International Journal on Cybernetics & Informatics (IJCI), vol. 3, no. 2, April

2014, pp. 11-20. AIRCC Publishing Corporation, India (2014). doi: 10.5121/ijci.2014.3202.

5. Abraham, S., Nair, S.: Cyber security analytics: a stochastic model for security quantification using absorbing Markov chains. In: Journal of Communications vol. 9, no. 12, December 2014, pp. 899-907. Engineering and Technology Publishing (2014). doi: 10.12720/jcm.9.12.899-907.
6. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q.: A survey of Game Theory as applied to Network Security. In: 43rd Hawaii International Conference on System Sciences, pp. 1-10. IEEE Computer Society Washington, DC, USA (2010). doi: 10.1109/HICSS.2010.35
7. Chung, K., A. Kamhoua, C. A., Kwiat, K. A., Kalbarczyk, Z. T., Iyer, R. K.: Game Theory with Learning for Cyber Security Monitoring. In: 17th International Symposium on High Assurance Systems Engineering (HASE), pp. 1-8. IEEE Computer Society Washington, DC, USA (2016). doi: 10.1109/HASE.2016.48.
8. Carin, L., Cybenko, G., Hughes, J.: Quantitative evaluation of risk for investment efficient strategies in cybersecurity: The queries methodology. In: IEEE Computer, pp. 1-18. AFRL/WS-07- 2145 (2007).
9. Zang, L. W., Yu, M.: Incentive-based modeling and inference of attacker intent, objectives, and strategies. In: ACM Transactions on Information and System Security (TISSEC) (2005).
10. Lye, K., Wing, J.: Game strategies in network security. In: Proceedings of the Foundations of Computer Security (2002).
11. Alpcan, T., Baser, T.: An intrusion detection game with limited observations. In: Proc. of the 12th Int. Symp. on Dynamic Games and Applications (2006).
12. Alpcan, T., Baser, T.: A game theoretic analysis of intrusion detection in access control systems. In: Proc. of the 43rd IEEE Conference on Decision and Control (2004).
13. Saad, W., Alpcan, T., Basar, T. and Hjorungnes, A.: Coalitional game theory for security risk management. In: 5th International Conference on Internet Monitoring and Protection (ICIMP '10), pp. 35–40. Washington, DC, USA (2010). doi: 10.11109/ICIMP.2010.14.