Securing System-of-Systems through a Game Theory Approach

Jamal El Hachem
IRISA – UMR CNRS / University of South Brittany
Vannes, France
jamal.el-hachem@irisa.fr

Elena Lisova
Mälardalen University
Västerås, Sweden
elena.lisova@mdh.se

Aida Čaušević
Mälardalen University
Västerås, Sweden
aida.causevic@mdh.se

ABSTRACT

Enabling System-of-Systems (SoS) security is an important activity when engineering SoS solutions like autonomous vehicles, provided that they are also highly safety-critical. An early analysis of such solutions caters for proper security architecture decisions, preventing potential high impact attacks and ensuring people's safety. However, SoS characteristics such as emergent behavior, makes security decision-making at the architectural level a challenging task. To tackle this challenge, it is essential to first address known vulnerabilities related to each *CS*, that an *adversary* may exploit to realize his attacks within the unknown SoS *environment*.

In this paper we investigate how to use Game Theory (GT) approaches to guide the architect in choosing an appropriate security solution. We formulate a game with three players and their corresponding strategies and payoffs. The proposal is illustrated on an autonomous quarry example showing its usefulness in supporting a security architect to choose the the most suitable security strategy.

KEYWORDS

Systems-of-Systems, Game Theory, Service Oriented Architecture, Security by Design, Autonomous Systems.

ACM Reference Format:
Jamal El Hachem, Elena Lisova, and Aida Čaušević. 2021. Securing System-of-Systems through a Game Theory Approach. In *The 36th ACM/SIGAPP Symposium on Applied Computing (SAC '21), March 22–26, 2021, Virtual Event, Republic of Korea.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3412841.3442125

1 INTRODUCTION

SoS are recognized as one of the major paradigms for engineering next generation solutions such as autonomous vehicles. SoS are composed of independent, evolutionary and distributed systems named as Constituent Systems (CS) that interact to achieve a higher global goal that none of the CS is able to accomplish in isolation [13]. In our work, we consider CSs as services, and the communication between CSs as a service per se. Securing these services and their interactions ensures the proper functioning of an SoS [10]. These complex services suffer from traditional security problems, in addition to those arising from SoS specific characteristics, and their emergent interactions leading to (un)expected behaviors [6].

When engineering an SoS, it is critical to first address known vulnerabilities related to each CS service, that an adversary may exploit and connect in known attack scenarios within an unknown SoS environment [7]. One way to address these vulnerabilities and attacks is by using suitable security mechanisms. Moreover, it is important to investigate the effectiveness of these mechanisms as soon as possible at the architecture level to avoid time and cost. However, a security architect usually lacks guidance to select the suitable security mechanism based on each architectural scenario (CS services interactions, known vulnerabilities and attacks but unknown environment). Thus, there is a need to provide an approach enabling comparison of the security mechanisms.

To this end, Game Theory (GT) is an analysis approach widely used for complex, distributed and critical systems [5]. In the context of SoS, GT aims at analyzing the independently operated and managed constituent systems. It focuses on situations in which interactions and inter-dependency play a significant role. In recent years, GT approaches where used to analyze complex systems security [3] and to study the critical decision-making situations of the defender and/or to analyze the motivations of the attackers [2, 3] by modeling the architecture and playing the game to execute it. Moreover, GT has been identified as a powerful tool to handle security issues in the autonomous vehicle's domain [8, 17].

Therefore, the this work has been motivated by the following Research Question (RQ): *How game theoretic approaches could be used to analyse SoS security and guide the security architect decision-making, such as choosing the most fit/advantageous security strategy based on the SoS services, possible known vulnerabilities, adversary/attack scenarios and unknown environment?*

To answer this RQ, we represent an SoS as a composition of services, that allows to consider behavior of an attacker, SoS vulnerabilities and security mechanisms possibly applied in the SoS. We formalize the triad via the GT approach by formulating a game with the corresponding players, strategies and payoffs.

The paper is organized as follows. Section 2 describes the proposed approach including players, strategy, and payoff formalisation. Section 3 investigates the related work for GT security analysis. The concluding remarks are presented in 4.

2 A PROPOSED GAME MODEL

The purpose of using game model and its execution within the security process for SoS is to assist risk assessment and following technical requirements elicitation. We assume that risk assessment

SAC '21, March 22–26, 2021, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-8104-8/21/03.
https://doi.org/10.1145/3412841.3442125

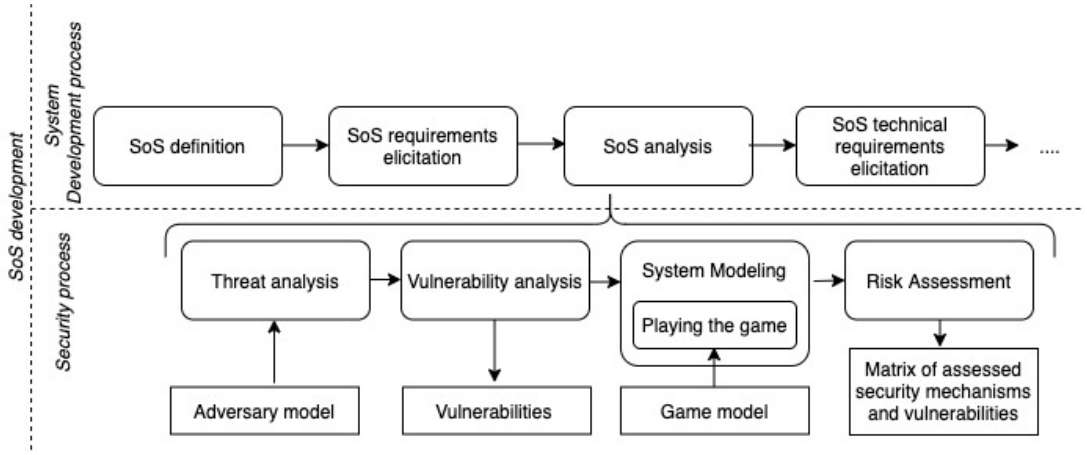

Figure 1: Game modelling in respect to SoS development

process is conducted based on Threat Assessment and Remediation Analysis (TARA) [1] the methodology where vulnerabilities and selected security mechanisms effective at mitigating those vulnerabilities, are assessed. The game outcome helps in choosing the most suitable security mechanisms and mitigation techniques to be used in SoS and captured by SoS technical requirements. Given the information regarding suitable countermeasures coming as the game outcome and knowledge about SoS vulnerabilities coming from the vulnerability analysis, it is possible to provide the list of recommended countermeasures and details on the effectiveness of each countermeasure over the range of vulnerabilities assessed.

Figure 1 illustrates our approach and its placement into the SoS development process. The game model is formulated based on: the SoS definition, i.e., its CSs, services and environment; an adversary model used for TARA; vulnerabilities discovered during a vulnerability analysis; and possible security mechanisms and mitigation techniques, that needs to be analyzed to determine their applicability and effectiveness for the SoS. The adversary model is not specified within TARA and is fed into the game model, however we can assume that an adversary is active, e.g., the HEAVENS model parameters for a threat level could be used as an adversary characteristics, namely expertise, its knowledge of the system under attack, available equipment, and window of opportunity combining access type and access duration [2].

The considered game can be classified as: not zero sum given that the payoffs are not defined to sum up to zero; dynamic as we look into the transition between the SoS state, i.e., considering deploying at least of few strategies from the corresponding player; and incomplete as we do not assume the attacker to be aware of the all the transitions rules of the system and as the SoS environment brings in an uncertainty/emergent behaviors.

To formulate the game model we introduce its main components: players, their strategies and associated payoffs. Further, we map the game state with the SoS states to define possible transitions and the game outcome. Once the model is defined, we illustrate the concept by instantiating the model and playing a round of the game.

[1]SAE J3061:2016, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems,
[2]https://autosec.se/wp-content/uploads/2018/03/HEAVENS_D2_v2.0.pdf

2.1 An overview of Game Theory

Game theory is a mathematical framework that allows to formally analyze possible interactions between game *players*, who are assumed to behave rationally, i.e., trying to optimize their *payoff*. Each play has a behaviour specified by a set of possible *strategies*, which together are forming a *strategy space*. The framework is used to investigate a decision-making process of a problem formulated as a game. Thus, a game formulated with valid assumptions helps to predict the outcome of players interaction and most probable behavior of players [18]. Formally a game, G, is defined by a number of players, N , their strategy spaces, S_i, and payoff functions, U_i: $G = \{N, S_1, .., S_N, U_1, .., U_N\}$ [11].

As the framework allows to consider parties with contradicting interest, the approach is widely used in analyzing interactions from a security standpoint [1]. Depending on application requirements, the game can be zero-sum if the payoffs of players are balanced and sum up to zero, dynamic or static depending on the number of rounds, and complete or incomplete depending on the knowledge of the players about each others' strategies and actions [14].

2.2 Formalisation of the players

Three players are considered in this game. The first actor is a SoS denoted as $Sys = \{CS_1, CS_2, \ldots, CS_n\}$, where n is a number of CS within the SoS. As an attribute each CS has a set of vulnerabilities $\{Vul_{k,i}\}$, where $i = 1..Vk$ and Vk is a number of vulnerabilities identified for k-th CS. Each vulnerability, $Vul_{k,i}$, has a severity parameter, $Sev_{k,i}$ indicating the scale of inflicted damage. We consider a discreet set of values for the severity: $Sev_{k,i} \in \{low = 1, medium = 2, high > 2\}$. The goal of this player is to prevent or minimize system disruption. The possible actions to take include deployment of security mechanisms and mitigation techniques. Sys can switch its state, three states were identified for the SoS:

- *Normal state* - SoS operate as expected, no suspicious behavior detected.
- *Quarantine state* - SoS are suspected to be under an attack, suspicious behaviour is being detected.
- *Under Attack state* - SoS are in preventive shutdown or isolation, a suspicious behaviour confirmed to be an attack.

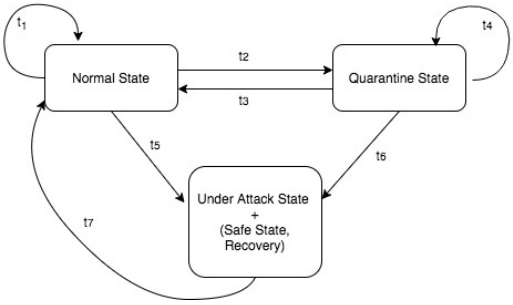

Figure 2: SoS states and transitions between them

The latter, implicitly includes switching into a safe mode and further system recovery. However, within the game we are interested only in what happens before the system is switched into the Under Attack state, as at this point we can estimate a security mechanism payoff. The states and transitions are illustrated in Figure 2.

The second player is an adversary, *Adv*, having the goal to cause maximum of disruption to *Sys*. *Adv* can deploy different attacks targeting vulnerabilities in CSs. Each attack, Att_i, exploits one or several vulnerabilities. As it was introduced above each vulnerability has a severity parameter, we calculate each attack impact, Imp_i, as the sum of related vulnerabilities severity. Consequently, the attack impact is also considered on the discrete scale: $Imp_i \in \{low = 1, medium = 2, high > 2\}$. We consider that the player succeeded if enough disruption have been caused, where enough is a threshold established in relation to the SoS assets value.

Finally, the last player is environment, *Env*. This player does not have a goal, however can impose disturbances that could be mistaken for attacks. *Env* is needed as a player to represent non-malicious faults in the system due to natural causes, i.e., it enables bringing safety aspects (failures without intent) to the game. Given that the Environment player brings an uncertainty as it can mask an attack or oppositely, provoke a false positive in detection an attack, it enables the use of the game theory as a tool due to it stops being a purely parametric situation.

2.3 Formalisation of the strategies

The game strategy space, S, is built upon strategies of each player, in the following way:

$$S = S_{sys} \times S_{adv} \times S_{env}, \tag{1}$$

where $\times$ is the Cartesian product, whereas S_{sys}, S_{adv}, S_{env} are respectively the strategy spaces of *Sys*, *Adv* and *Env*.

The SoS strategy space consist of combinations of its possible states and security mechanisms and mitigation techniques available to be deployed, for simplicity reasons both security mechanisms and mitigation techniques are denoted as *Mech*:

$$S_{sys} = \{\{S_{sys}^{Nor}, S_{sys}^{Qua}, S_{sys}^{UAt}\} \times \{Mech_1, ..., Mech_P\}\}, \tag{2}$$

where S_{sys}^{Nor}, S_{sys}^{Qua}, and S_{sys}^{UAt} are respectively the Normal, Quarantine and Under Attack states of SoS, while P is the number of mechanisms (including mitigation techniques) available for the SoS. Thus, each system state can be associated with a sub-set of available security mechanisms deployed in this state. Each mechanism, $Mech_i$, has a cost, $Cost_{mech,i}$, and consequently a cost, $Cost_Mech_x$, of a SoS state X having deployed a M_x security mechanism, is defined as:

$$Cost_Mech_x = \sum_{i=1}^{M_x} Cost_{mech,i}. \tag{3}$$

Moreover, each mechanism, $Mech_i$, has a parameter called deployment time, $DepTime_{mech,i}$, by which we understand the time required to kick in and react. We propose to assess this parameter in a qualitative manner like $slow/fast$, as it is enough o compare mechanisms between each other in the first estimation.

The adversary strategy space consists of a set of available attacks:

$$S_{adv} = \{Attack_1, Attack_2, ..., Attack_N\}, \tag{4}$$

where N is a number of attacks available for the adversary. Each attack, $Attack_i$, has an associated cost, $Cost_{att,i}$. Thus, each SoS state can be associated with the summary cost of the attacks being deployed by the adversary at this moment:

$$Cost_Att_x = \sum_{i=1}^{A_x} Cost_{att,i}, \tag{5}$$

where A_x is the amount of the attacks being deployed in the SoS state X.

Finally, the third player, *Env*, can impose natural disturbances, its strategy space is defined as:

$$S_{env} = \{Dist_1, Dist_2, ..., Dist_K\}, \tag{6}$$

where K is the amount of existing disturbances. This player, does not have a goal and thus there is no associated cost for a chosen strategy. To choose when a disturbance is happening, a relevant probability distribution is used.

Each disturbance has its cost for SoS, $Cost_{dist,i}$. Thus, each SoS state can be associated with the summary cost of disturbances being deployed by environment:

$$Cost_Dist_x = \sum_{i=1}^{D_x} Cost_{dist,i}, \tag{7}$$

where D_x is the amount of the disturbances being deployed in the SoS state X.

2.4 Definition/attribution of the Payoffs

We assume the pay-off to be expressed in terms of being Pareto optimal [4]. The outcome of the game is Pareto optimal if there is no other outcome that makes every player at least as well off and at least one player strictly better off. Meaning it is not possible to improve a Pareto optimal outcome without hurting at least one player (i.e., if a strategy of *Sys* on securing the system is successful its pay-off increases while *Adv* gets lower pay-off since its strategy is obviously not working. For simplicity let us assume 2 players (p_1 and p_2) in the game, formally the pay-off function U for a game outcome d' is defined as follows:

$$\begin{aligned}[u_{p_1}(d') \geq u_{p_1}(d) \wedge u_{p_2}(d') \geq u_{p_2}(d)] \wedge \\ [u_{p_1}(d') > u_{p_1}(d) \vee u_{p_2}(d') > u_{p_2}(d)].\end{aligned} \tag{8}$$

Let us assume that SoS is in the state X and that in this state in total for all CSs V_{sum} vulnerabilities is exploited, then the SoS

payoff, $Payoff_{Sys}$, and the adversary payoff, $Payoff_{Adv}$, could be calculated as following:

$$Payoff_{Adv} = Sev_{k,i} - Cost_{A_x}, \tag{9}$$

$$Payoff_{Sys} = -Cost_{S_x} - Cost_{D_x} - Sev_{k,i}. \tag{10}$$

Payoffs defined in such matter satisfy Pareto definition (Eq. 8), which eases game outcome interpretations for the following up risk assessment.

3 RELATED WORK

Game theoretic approaches play an important role in security decision makings and adversarial attacks fight as shown by several studies presented and discussed below.

Dasgupta et al. [2], reviewed the approaches that use GT for making machine learning techniques robust against adversarial attacks. The authors identified several open problems such as building richer models to cover the interdependent system interactions and taking into account adversary limitations.

In another survey [3], authors overview the theoretical games used for cyber-physical security, communication security, and privacy. They identified Internet-of-Things devices and Device-to-Device communications among the future directions of game-theoretic approaches for cybersecurity.

Three other surveys discussed the importance of using GT for guiding the security analyst decision making. [9] surveys GT approaches for independent information systems where the CSs are not only dependent on their own security, but are also impacted by the security-related decisions of others. The survey focuses on games with interdependent defenders and do not present two-player attacker-defender games. [15] surveys GT approaches used for network security, where security is modeled by two players: the attacker and the defender, each trying to attend its objective. In [12] authors argue the usefulness of security games in providing a scientific basis for high-level security-related decision making in computer and communication networks.

Similarly, Sinha et al. [16] considered the use of security game to study interactions between the defender and adversary to handle real-world security challenges.

In a study closer to our work, Ilavendhan et al. [8] suggested the general use of GT as a promising approach for mitigating various attacks in different type of VANET. However, authors have not discussed neither how the security game should be modeled, nor how the game should be played to identify the best security mitigation.

4 CONCLUSION

SoS specific characteristics and complexity arising from the uncertainty of behavior generate many engineering challenges related to the SoS system properties, in particular safety and security. However, security decision making is not a trivial task. One of the main reason is that the defender's strategies are impacted by those of the attacker's and by the SoS environment disruptions. Therefore, a careful analysis of the optimal security strategies is of crucial importance to protect against potential attacks.

To address these challenges, we propose a GT approach allowing the analysis of the SoS architecture and its security, to support the early decision making when selecting the most beneficial security countermeasure to be designed. To do so, we formalise a security game allowing to analyze the conflict between the CS and the adversary players trying to maximize their individual benefits within the SoS environment that we represent as a third player. In this game, the players can pick and apply a strategy from a set of various behavioral options, in order to maximize the payoff they are gaining as an outcome of the game.

ACKNOWLEDGEMENTS

This work is supported by the Serendipity project funded by SSF.

REFERENCES

[1] William Casey, Ansgar Kellner, Parisa Memarmoshrefi, Jose Andre Morales, and Bud Mishra. 2018. Deception, Identity, and Security: The Game Theory of Sybil Attacks. *Commun. ACM* 62, 1 (Dec. 2018), 85–93. https://doi.org/10.1145/3190836

[2] Prithviraj Dasgupta and Joseph Collins. 2019. A Survey of Game Theoretic Approaches for Adversarial Machine Learning in Cybersecurity Tasks. *AI Magazine* 40, 2 (2019), 31–43. https://doi.org/10.1609/aimag.v40i2.2847

[3] Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, Shaolei Ren, Niki Pissinou, and Sundaraja Sitharama Iyengar. 2017. Game Theory for Cyber Security and Privacy. *ACM Comput. Surv.* 50, 2 (2017), 37. https://doi.org/10.1145/3057268

[4] Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, Shaolei Ren, Niki Pissinou, and Sundaraja Sitharama Iyengar. 2017. Game Theory for Cyber Security and Privacy. *ACM Comput. Surv.* 50, 2, Article 30 (May 2017), 37 pages. https://doi.org/10.1145/3057268

[5] Thilo Gross and Bernd Blasius. 2007. Adaptive coevolutionary networks: a review. *Journal of The Royal Society Interface* 5, 20 (2007), 259–271. https://doi.org/10.1098/rsif.2007.1229

[6] Jamal EL Hachem, Vanea Chiprianov, Muhammad Ali Babar, Tarek AL Khalil, and Philippe Aniorte. 2020. Modeling, analyzing and predicting security cascading attacks in smart buildings systems-of-systems. *Journal of Systems and Software* 162 (2020), 110484. https://doi.org/10.1016/j.jss.2019.110484

[7] J. EL Hachem, Z. Pang, V. Chiprianov, A. Babar, and P. Aniorte. 2016. Model Driven Software Security Architecture of Systems-of-Systems. In *Proceedings of the 23rd Asia-Pacific Software Engineering Conference (APSEC)*.

[8] A. Ilavendhan and K. Saruladha. 2018. Comparative study of game theoretic approaches to mitigate network layer attacks in VANETs. *ICT Express* 4, 1 (2018), 46 – 50. https://doi.org/10.1016/j.icte.2017.12.002 SI: CI & Smart Grid Cyber Security.

[9] Aron Laszka, Mark Felegyhazi, and Levente Buttyan. 2014. A Survey of Interdependent Information Security Games. *ACM Comput. Surv.* 47, 2, Article 23 (Aug. 2014), 38 pages. https://doi.org/10.1145/2635673

[10] Elena Lisova, Jamal El Hachem, and Aida Causevic. 2019. Investigating Attack Propagation in a SoS via a Service Decomposition. In *IEEE SERVICES Workshop on Cyber Security and Resilience in the Internet of Things*.

[11] Patrick Maillé, Peter Reichl, and Bruno Tuffin. 2011. *Of Threats and Costs: A Game-Theoretic Approach to Security Risk Management.* Springer New York, New York, NY, 33–53.

[12] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. 2013. Game Theory Meets Network Security and Privacy. *ACM Comput. Surv.* 45, 3, Article 25 (2013), 39 pages. https://doi.org/10.1145/2480741.2480742

[13] Claus Ballegaard Nielsen, Peter Gorm Larsen, John Fitzgerald, Jim Woodcock, and Jan Peleska. 2015. Systems of Systems Engineering: Basic Concepts, Model-Based Techniques, and Research Directions. *ACM Comput. Surv.* 48, 2, Article 18 (Sept. 2015), 41 pages. https://doi.org/10.1145/2794381

[14] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu. 2010. A Survey of Game Theory as Applied to Network Security. In *43rd Hawaii International Conference on System Sciences*. 1–10. https://doi.org/10.1109/HICSS.2010.35

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

[16] Arunesh Sinha, Thanh H. Nguyen, Debarun Kar, Matthew Brown, Milind Tambe, and Albert Xin Jiang. 2015. From physical security to cybersecurity. *Journal of Cybersecurity* 1, 1 (11 2015), 19–35. https://doi.org/10.1093/cybsec/tyv007

[17] Basant Subba, Santosh Biswas, and Sushanta Karmakar. 2018. A game theory based multi layered intrusion detection framework for VANET. *Future Generation Computer Systems* 82 (2018), 12 – 28. https://doi.org/10.1016/j.future.2017.12.008

[18] M. Wooldridge. 2012. Does Game Theory Work? *IEEE Intelligent Systems* 27, 6 (Nov 2012), 76–80. https://doi.org/10.1109/MIS.2012.108