GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments

Ioannis Kalderemidis
kalderemidis@ssl-unipi.com
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

Aristeidis Farao*
arisfarao@unipi.gr
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

Panagiotis Bountakas
bountakas@unipi.gr
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

Sakshyam Panda
s.panda@greenwich.ac.uk
School of Computing and
Mathematical Sciences,
University of Greenwich
Park Row, London, United Kingdom

Christos Xenakis
xenakis@unipi.gr
Department of Digital Systems,
University of Piraeus
Piraeus, Greece

ABSTRACT

Investments on cybersecurity are essential for organizations to protect operational activities, develop trust relationships with clients, and maintain financial stability. A cybersecurity breach can lead to financial losses as well as to damage the reputation of an organization. Protecting an organization from cyber attacks demands considerable investments; however, it is known that organisations unequally divide their budget between cybersecurity and other technological needs. Organizations must consider cybersecurity measures, including but not limited to security controls, in their cybersecurity investment plans. Nevertheless, designing an effective cybersecurity investment plan to optimally distribute the cybersecurity budget is a primary concern.

This paper presents GTM, a methodology depicted as a tool dedicated to providing optimal cybersecurity defense strategies and investment plans. GTM utilizes attack graphs to predict all possible cyber attacks, game theory to simulate the cyber attacks and 0-1 Knapsack to optimally allocate the budget. The output of GTM is an optimal cybersecurity strategy that includes security controls to protect the organisation against potential cyber attacks and enhance its cyber defenses. Furthermore, GTM's effectiveness is evaluated against three use cases and compared against different attacker types under various scenarios.

KEYWORDS

Cybersecurity investments, Game Theory, Attack Graphs, Budget Allocation, Risk Estimation

1 INTRODUCTION

Modern systems are targeted by sophisticated adversaries that identify vulnerabilities in different components of systems and cleverly allocate their endeavors to compromise the whole organization. In 2021, 21,957 vulnerabilities have been revealed showing a raise of 19.57% compared with 2020 [8], where, in the period July-September 2021, zero-day exploits were accountable for 67.2% of malware[6]. Moreover, email attacks (e.g., phishing) have seen a 64% rise during the last couple of years due to COVID-19 [4]. Phishing attacks constitute the first step towards more complex and large-scale attacks, such as Exploit Kits [5], which are attacks that exploit vulnerabilities in web browsers and silently (i.e., without draw users attention) deliver malware to victims' or Advance Persistent Threats [33], which are attacks that establish an illicit and long-term presence on a network. In [21], the authors have highlighted the fact that the use of vulnerable Node.js functions can lead to Server-Side JavaScript Injection attacks compromising the web servers that execute the JavaScript code resulting in catastrophic consequences for an organization.

On the other hand, one of the most pressing issues that organizations face nowadays is to manage cyber risks, which involves protection [2, 3, 11, 17, 27, 34], mitigation [4, 12, 26, 30] and insurance [10, 24, 28]. The most common reason that hinders this process is the limited budget. The cybersecurity enhancement of an organization's network goes much beyond simply identifying and patching its known flaws towards understanding the behavior of attackers [25]. Although there are numerous solutions that can assist Chief Information Security Officers (CISOs) figure out which parts

of a network are vulnerable (e.g., [31], [37]), these solutions do not take into account other important parameters. For instance, what conditions and requirements might affect the state of the system during a security incident, and how people act inside and outside the network, which toughens the optimal countermeasure identification procedure. Furthermore, organizations face constraints including the limited budget and resources that necessitate making judgments that sometimes require keeping some risks.

Based on the above-mentioned statements, the motivation for this work stems from the need of organizations to strengthen their defenses against cybersecurity threats as well as from the CISOs' concern regarding the allocation of a limited budget to attain optimal protection. While organizations aspire to economically and technologically blossom in the new digital era, cybersecurity professionals have to cope with new threats and efficiently protect the organizations from sophisticated attackers who aim to evade the organizations' defenses. The main challenges that cybersecurity professionals face are summarized below:

(1) Limited cybersecurity budget: Contrary to popular belief, corporations seldom attach importance to spending on cybersecurity. While cybersecurity concerns have risen to the top of the priority list, CISOs continue to struggle to get greater budgets, frequently because they cannot demonstrate a clear return on investment. When it comes to appropriately mitigate hazards, budget constraints are often a problem for organizations.
(2) Multilevel cybersecurity threats: Organizations struggling to follow the latest technological advances create a fertile surface full of cybersecurity and third-party threats that can be exploited by attackers.
(3) Cybersecurity results communication: Employees often are not informed about all components of the security program that affect their working-routine as well as they are not aware of the cybersecurity risks in case they are not familiar with the principles of safe cybersecurity practices rendering them the weakest link in a cybersecurity attack.

Considering the aforementioned motivation and challenges, this paper proposes a methodology that is presented as a software tool, named GTM. The latter exploits attack-graph and game theory methods to automatically provide cybersecurity defensive strategies, including security controls that can mitigate the cybersecurity risk of an organization in a scenario agnostic manner (i.e., One organization with multiple attackers). More specifically, the attack graphs are used in GTM to shape all multi-stage attack paths. Each path portrays a collection of exploits that could be leveraged by an attacker to compromise a network. The interactions between the Attacker and Defender during a cybersecurity incident are treated as a zero-sum game, which is solved using the Nash equilibrium method. In particular, GTM achieves to sculpt the attackers' and defenders' behavior and their strategies. Moreover, the integration of GTM in an organization's working routine can facilitate CISOs to optimally allocate the limited cybersecurity budget to the most appropriate security controls based on the organization's needs.

In summary, the contribution of this work lies in the following aspects:

- We introduce a methodology and its implementation as a software tool to facilitate security managers identifying the most appropriate defensive strategies regardless of the organization's environment.
- We automatically calculate the optimal allocation of the limited cybersecurity budget of an organization.
- We effectively combine attack graphs and game theory for the generation of an optimal budget allocation plan.
- We evaluated the proposed tool against three realistic case studies proving its effectiveness in real-life working environments.

The paper unfolds as follows: Section 2 presents essential information regarding state-of-the-art works in optimal budget allocation and attack graph fields. Next, Section 3 elaborates on the processes of the GTM tool describing in detail the architecture and its technical details. Section 4 includes a quantitative and qualitative performance evaluation of GTM proving that stands well on different attacking surfaces. Finally, Section 5 concludes the paper.

2 RELATED WORK

This section delves into the literature focusing mostly on the domains of optimal budget allocation and attack graphs, which are the two key domains that the proposed work combines.

2.1 Optimal Budget Allocation

Panaousis et al. [23] introduced a methodology to facilitate security managers performing an optimal cybersecurity budget allocation. The methodology begins by conducting a risk analysis of the organization's assets and analyzing the efficacy of various security controls against known vulnerabilities. Then, the authors calculate the most optimal way for an organization to implement each control based on control games. The control game is a method to assist a defender to reduce cybersecurity risks by adopting a game-theoretic approach based on Nash Equilibrium that decides how a control will be implemented. The authors treat the problem of the optimal allocation of a cybersecurity budget as a multi-objective Knapsack problem. Finally, to implement the proposed methodology, a case study of an SME has been considered employing 12 of the topmost dangerous vulnerabilities from the 2011 CWE/SANS report[1] as well as 6 critical security controls published by the Council on Cybersecurity[2].

An extension of [23] presented in [12], where Fielder et al. proposed a two-stage model to aim security professionals with decisions considering the optimal cybersecurity budget allocation. The authors begin by formulating the environment, where the cybersecurity investments will occur, identifying the targets that an attacker has as well as the defenses of these targets. The environment was later deployed to define control games based on Nash equilibrium. To conclude the optimal budget allocation the problem was formalized as a multi-objective Knapsack problem. The proposed model was compared with two alternative methods, namely with two scenarios that aim to enhance the defense using

[1] http://cwe.mitre.org/top25/
[2] http://www.counciloncybersecurity.org/attachments/article/12/CSC-MASTER-VER50-2-27-2014.pdf

direct costs and indirect costs. Finally, the authors highlight the impact that indirect costs have on the cybersecurity budget allocation problem.

Towards this direction, Panda et al. [26] focus on the optimal selection of cyber-hygiene controls to minimize the risk of cyber-attacks. To achieve their goal, a tool for the optimal selection of safeguards has been proposed, which combines game theory and combinatorial optimization considering the attack probability, the asset value, and the efficacy of each control. In [38], Wang introduced an analytical framework for organizations to improve their cybersecurity and cyber-insurance investments. The framework is based on analytical models to quantify the effect of security investments in tackling cyber threats, vulnerability, and impact on the budget. A limitation of this work is that the organizations need to evaluate their security investment in a long-term multi-period.

Another recent work that focuses on the budget allocation for data privacy protection is proposed in [9]. Particularly, the paper focuses on the improvement of the privacy budget allocation in differential private clustering algorithm DPk-means by introducing a new algorithm named APDk-means, which is based on arithmetic progression privacy budget allocation. The novelty of APDk-means is that it achieves rapid convergence in early iteration by decomposing the total budget into a decreasing arithmetic progression to distribute the privacy budgets from large to small in the repetitive procedure. The evaluation showed that APDK-means accomplished better availability and quality performance and the same privacy protection level in comparison with other deferentially private k-means models.

Previous works that focus on cybersecurity budget allocation mostly focus on a scenario where an attacker has a single target in an organization, neglecting to consider attackers with multiple targets. An attacker that aims to exploit multiple assets represents a more realistic threat scenario for an organization, hence the applicability of these works to real-life situations is uncertain. GTM addresses this gap by integrating a game-theoretic approach with attack graphs to optimally allocate the cybersecurity budget considering multiple attacks.

2.2 Attack Graphs

The generation of attack graphs is a technical approach that demands the collection of assets and vulnerabilities. We can observe that with the increasing number of cyberattacks and the fact that vulnerabilities threaten more than one asset, the complexity of an organization's topology increases exponentially. The automatic generation of attack graphs can be broadly classified into four categories [31], as highlighted below:

(1) **Enumeration Based:** The nodes display the condition of the network during an attack, as well as the entities that are participating in the cyber attack.
(2) **Topological vulnerability analysis (TVA):** It concentrates on the system's vulnerabilities. The attacker's options for compromising the targeted network assets are then defined after the found vulnerabilities have been analyzed.
(3) **Network Security Planning Architecture (NetSPA):** It analyzes the network topology identifying the most critical attack pathways. It is a multi-prerequisite graph with nodes for the state, preconditions, and vulnerabilities allowing the network owner to locate and rectify the network's most vulnerable aspects.
(4) **Logic Programming:** It demonstrates the logical relationships between attack objectives and configuration information. Multi-host, Multi-stage, Vulnerability Analysis Language (MulVAL) [22] is a well-known tool that is based on this approach. MulVAL adopts the Datalog modeling language to analyze the elements of a network leveraging existing vulnerability DBs (e.g., NVD) and scanning tools.

Wang et al. [37] developed a framework to link vulnerability analysis with risk assessment. The framework is based on attack graphs to represent network assets and vulnerabilities and Hidden Markov Models to capture the uncertainties of those explicit observations and estimate attack states, which vary based on the cost that is related to possible attacks and countermeasures.

In [31] the authors proposed a methodology based on probabilistic attack graphs to objectively measure the security risk of organizations. The authors deployed MulVAL for the generation of attack graphs and the CVSS standard to assess the severity of the vulnerabilities.

Kotenko et al. [15] presented and demonstrated a case study risk assessment technique that is based on attack graphs to be implemented in SIEMs. The crux of this work is the developed metrics taxonomy that considers the latest trends in the security metrics domain, the translation of attack steps to attack graphs, and the purposes and results of SIEMs.

The authors in [1] focus on game-theoretic security investments of multiple interdependent assets. The interdependencies between the assets have been modeled using attack graphs, where the edges linking two assets (vertices) contain the probability of a successful pivot. The authors concluded that the human decision-making process (based on the behavioral probability weighting) can have a significant effect on interdependent systems' security.

The article in [29] utilizes attack graphs to elaborate on the attack prediction. To attain their goal the authors first identify all the possible attack paths and then deploy the attack paths combined with common vulnerability data for future attack prediction. The efficacy of the method is evaluated on real data from a maritime supply chain infrastructure showing that is both practical and effective.

An extension of MulVAL [22], which is a popular tool for attack graph generation (see section 3.2), proposed in [32] to support network protocol vulnerabilities and support advanced communication types. Particularly, this work considers the physical network topology, implements short-range communication protocols, models vulnerabilities of network protocols, and considers particular industrial communication systems. The authors demonstrate that their extension can model several well-known network attacks, such as spoofing, man-in-the-middle, and DoS as well as attacks on industrial communication systems.

Attack graphs have been proved to be very effective in vulnerability detection and attack prediction domains. However, previous works did not deploy attack graphs on the optimal budget allocation domain. Thus, in this paper, the effectiveness of attack graphs has been exploited to predict all the possible attack scenarios on

an organization and conclude the best allocation of the budget to enhance the resilience of the organization against cyberattacks.

3 GTM

3.1 GTM Overview

The proposed cybersecurity investment tool, named GTM, aims to greatly facilitate from top to bottom members of cybersecurity Blue and Red Teams, including but not limited to CISOs, C-Suite executives, Security and Information Technology Analysts, Board of Directors of an organization and Security Researchers. To assist the reader to understand the presented notions, CISO is assumed as the end-user of GTM; however, we avoid analyzing CISO's responsibilities and requirements since it is out of the scope of this work. Through GTM, all possible attacking scenarios will be predicted by employing attack graphs, and then utilizing game-theoretic techniques optimal defending strategies will be proposed achieving optimal cybersecurity budget allocation for cybersecurity risk mitigation.

As shown in Figure 1, the general structure of GTM is divided into three main modules: i) the Attack Graph Engine; ii) the Data Pool, and iii) the Defense Strategy. The **Attack Graph Engine** as its name implies is responsible to generate attack graphs that model all possible attacking scenarios and paths of an organization. It receives as input a vulnerability assessment report that is the output of a vulnerability assessment tool (e.g., Nessus [36]). The **Data Pool** contains numerous guidelines, laws, and reports related to cybersecurity and privacy, which are used to defend organizations against cyber attacks. In addition, it is utilized as a database and is enriched with new input by CISOs whenever it is necessary (e.g., when a new cybersecurity incident occurs). Finally, the **Defense Strategy** is the most important pillar of GTM as it is responsible not only to calculate the expected loss but also to choose the most appropriate cybersecurity controls optimally allocating the limited cybersecurity budget. In particular, it simulates cyber attacks following the game theory and random attacker's profile to calculate the probability of occurrence of any cyber attack leading to the optimal budget allocation.

The game-theoretic approach that is implemented in the Defense Strategy is scenario agnostic. This characteristic is inherited by the zero-sum game; GTM is capable to support games that include one organization as the Defender and multiple opponents as Attackers. With such an approach, CISOs can utilize GTM in numerous attacking scenarios, where attackers have at least one target to compromise. Also, GTM stands not only against technical vulnerabilities (e.g., CVEs) that usually could be mitigated following patching approaches provided by vendors, but also against physical and environmental vulnerabilities (e.g., air-conditioning failure) that are also able to lead to catastrophic consequences affecting business continuity.

3.2 Attack Graph Engine

GTM has been equipped to construct attack graphs with the commonly used Multi-host, Multi-stage Vulnerability Analysis Language, often known as MulVAL, which is a Logic Programming attack graph tool [22]. The produced graph (see Figure 2) is comprised of nodes that represent logical propositions, and it requires

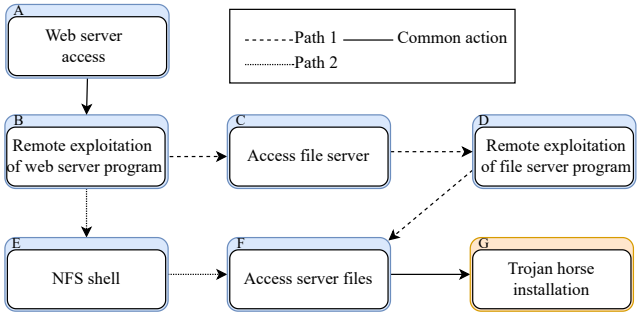

Figure 1: GTM blueprint

that the source of an attacker's potential privileges be expressed as a propositional expression in terms of network configuration parameters. In a MulVAL graph (see Figure 2), a rectangle represents the current state of the system, whether it is an antivirus defending a specific host or the presence of a threat. Additionally, the circular one denotes the pre and post-conditions of an attack being connected with diamond shapes. The latter depicts the attacker's potential advantage.

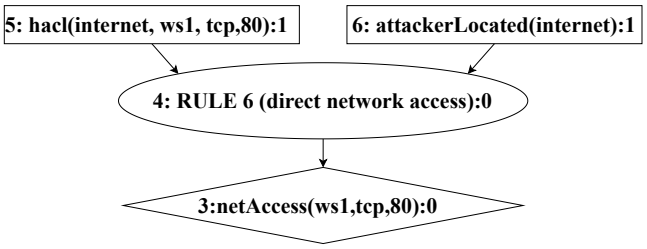

Figure 2: Toy-example of a MulVAL attack tree

GTM has the following requirements regarding the utilized attack graph approach: i) being open-source; ii) limited complexity, namely, an attack graph should scale well regardless of the size of the organization network; iii) scalability to Small Office/Home Office (SOHO), a situation that became norm and trend for many professionals due to the working from home situation as a result of COVID-19; iv) the applicability to Small Medium Enterprises (SMEs) since this type of organization is the backbone of Europe's economy [7], and v) the applicability to Large Enterprises (LE) since LE might be susceptible to a large number of vulnerabilities (e.g., CVE) due to the number of devices and application they include to their daily working-routine [10]. Table 1 compares the attack graph generation approaches analyzed in Section 2 against the aforementioned features. For the comparison, we replaced enumeration-based attack graphs approach, since it has been considered as obsolete, with the Attack Graph Toolkit [40] that creates attack graphs and is the closest to the enumeration-based approach architecture. The Attack Graph Toolkit and MulVAL are open-source and available for free. The most efficient complexity can be found by NetSPA. The Attack Graph Toolkit can handle SOHO environments, its scalability in an SME environment depends on the number of assets; however, it is a suitable approach for an LE environment. The performance

of TVA depends on the number of the identified assets regardless of the working environment. NetSPA and MulVAL can scale well regardless of the working environment. Overall, the most appropriate methods for GTM are NetSPA and MulVAL; however, GTM integrates MulVAL due to its open-source characteristic.

3.3 Defense Strategy

3.3.1 Risk estimation. As previously stated, attack graphs are constituted of nodes and edges that depending on the graph creation method used, provide a distinct interpretation of the current state of the system. In most cases, attackers exploit these stages as a launching pad to infiltrate their intended target. After figuring out these flaws, a CISO has to decide which defense mechanisms are most important for the network. In this section, a method for evaluating the nodes and possible controls has been provided that will eventually compose an effective network defense.

GTM aims at estimating the expected loss L of an organisation as well as to assist in acquiring an optimal selection of safeguards using game theory. We denote $\mathcal{A}$ the set of assets, which belongs to an organisation O and express each asset as a, where $a \in \mathcal{A}, \mathcal{A} \in \mathbb{Z}_n^+$. Each asset a is characterized by an impact value I_a, which is displayed in monetary units. The value of I_a is defined by CISO's organization and derives from a Business Impact Analysis (BIA). We express P_a as the probability of occurrence of a threat to a specific asset a, where $P_a = [0, 1]$; $P_a \in \mathbb{R}$ [19], also, denote the probability of a successful exploitation of a cyber attack to an asset a as $R_a = [0, 1]$; $R_a \in \mathbb{R}$ [39]. We measure the expected loss L using the commonly-used risk assessment equation containing the likelihood of a threat event's occurrence (P_A), the likelihood of successful exploitation of the target (P_{SA}), as well as the potential impact of the successful exploitation (I) [20], as it is displayed in Equation 1.

$$L = P_A \times P_{SA} \times I \tag{1}$$

In GTM the total expected loss is calculated based on threats that may occur to the assets. We assume that each asset is connected with numerous threats. GTM defines the expected loss that derives from the Equation 1 expressing it in monetary units, achieving a quantitative result. Hence, the total expected loss L is given by the sum of the maximal expected losses [35]. The L_a expresses the expected loss associated with a specific asset a. Moreover, we define the $L_{a,i}$ as the expected loss associated with a specific asset a and a specific threat i, $i \in \mathcal{T}$, where $\mathcal{T}$ is the set of treats that can impact the organization O. The total expected loss L_O of an organization is calculated as it is presented in the Equation 2.

$$L_O = \sum_{a \in \mathcal{A}} L_a \tag{2}$$

However, to integrate the defensive approach in GTM, we take into consideration the parameter $\mathcal{S}$ that represents the level of security provided by a defensive approach. It is calculated by $\mathcal{S} = 1 - e$, where e expresses the efficacy of the implemented control. Finally, the total cybersecurity expected loss is calculated based on the Equation 3.

$$L_O = \sum_{a \in \mathcal{A}} L_a = \sum_{a \in \mathcal{A}} I_a \prod_{i \in \mathcal{T}} P_{i,a} \times R_{i,a} \times S_{i,a} \tag{3}$$

3.3.2 Security Investments. CISOs can integrate into GTM security controls to defend against an Attacker, who acts based on a game-theoretic approach. This is represented as a game between two players, the Defender and the Attacker [16]. On the one hand, the Defender chooses the security control that will be implemented on a specific asset; however, the integrated security control does not provide full protection against all threats. The game that is created in GTM is a zero-sum game that is solved using the Nash equilibrium approach. Since, if one player loses, the other party wins, and the net change in wealth is zero. For instance, if an attacker achieves to compromise the organization's network then he will win and get benefited from the loots; however, the organization will lose wealth including assets (e.g., confidential data), money and reputation. On the other hand, the Attacker chooses to attack a specific asset a that she assumes to be more susceptible to specific vulnerabilities. The Attacker is in a dilemma without knowing the next attacking step (e.g., exploiting a vulnerability) which is depicted by the attack graph by splitting into more than one discrete path. In particular, the game-theoretic approach has a close connection with the probability of occurrence of an attack. In this paper, we will determine the occurrence probability of a threat as the attacker's payoff considering that is equal to the vulnerability's CVSS [13] score. CVSS stands for Common Vulnerability Security Score, and has been chosen since it depicts how a vulnerability (CVE) can be exploited (i.e., attack vector, attack complexity, privileges required, user interaction) as well as how its exploitation impacts the organization (i.e., confidentiality impact, integrity impact, availability impact). On the one hand, the Attacker's payoff is considered the CVSS score. On the other hand, the Defender is divided into two discrete instances: i) the first one is the Defender, who does not implement any security control, then his payoff is equal to the negative CVSS score and ii) the second one is the Defender who implements security controls, then his payoff is equal to the aggregated result of CVSS score and the cost that is required to implement the security control.

During the integration of each security control, there will be an economic influence (e.g., cost) on the organization. The cost can be categorized as followed: i) in *Direct Cost* that is a one-time investment that is required for the control to be purchased and ii) in *Indirect Cost* that is not directly accountable to a cost object (e.g., maintenance issues). Security control usually fall into both categories. A control commonly requires a direct cost for its purchase as well as an indirect cost for its maintenance; the total cost of a security control can be calculated by Equation 4.

$$Cost_{total} = Cost_{direct} + Cost_{indirect} \tag{4}$$

The last feature of GTM is the optimal allocation of a limited budget. To achieve it, GTM utilizes the 0-1 Knapsack problem. The latter is a combinatorial optimization problem in which we must identify the combination of items that will generate the highest value within a specific total weight limit, given a collection of objects each with a weight and a value. However, when it comes to network security, the method differs according to resource interaction and the degree to which resources are divided equally among

Table 1: Caption

Attack Graph Approach	Open-source	Scalability	SOHO	SME	LE
Attack Graph Toolkit	✓	Exponential	✓	# assets	✗
TVA	✗	$O(N^3)$	# vulnerabilities	# vulnerabilities	# vulnerabilities
NetSPA	✗	$O(NlogN)$	✓	✓	✓
MulVAL	✓	$O(N^2) \sim O(N^3)$	✓	✓	✓

the targets. The 0-1 Knapsack problem integrated with GTM consists of two parameters: i) the Weight that is equal to the loss that occurred to the system due to the exploitation of a specific vulnerability (i.e. CVE) and is calculated based on Equation 3 and ii) the Cost that depicts the total costs of security control, it is calculated based on Equation 4.

4 CASE STUDY

In this section, we aim to examine the applicability of GTM to three discrete case studies: i) the first case study represents a SOHO that seeks a defensive strategy against an Attacker who has only one target; ii) the second case study represents an SME that aims to protect itself against an Attacker who has multiple targets (e.g., multiple assets of the SME), and iii) the third case study refers to an SME that aims to find a strategy to protect itself not only from technical vulnerabilities but also from vulnerabilities that impact its physical and environmental security. The experiments were performed in an Ubuntu 18.04 desktop PC equipped with a Quad-Core Processor at 3.2GHz (AMD Ryzen 5 1400) and 8GB RAM. For the implementation of GTM, we have developed our code in Python language. The main goal of our experiments is to determine that GTM can effectively work in numerous different working environments.

4.1 Attacker with one target

This case study as it is shown in Figure 3 consists of two discrete paths. The attacker aims to remotely install a Trojan horse on the file server. Each node represents a system vulnerability that can be exploited by the Attacker, it also can be partially protected and prevented by implementing certain countermeasures by the Defender. We assume that the CISO has to handle a budget of the 100 monetary units, the efficacy on each node has been set at 0.5. Moreover, the following costs have been set for the security controls of each node to prevent a post-condition step: $C_{(b,c)} = 40$, $C_{(c,d)} = 20$, $C_{(d,f)} = 5$, $C_{(b,e)} = 60$, $C_{(e,f)} = 35$ and $C_{(f,g)} = 120$. Furthermore, the probability of an attack to be successfully executed has been befined as follows, $P_{(b,c)} = 0.64$, $P_{(c,d)} = 0.51$, $P_{(b,e)} = 0.64$, $P_{(e,f)} = 0.51$ and $P_{(f,g)} = 0.53$. At this point, it should be noted that the aforementioned values are arbitrary. The participants of this case study are the following: i) Game Theory attacker: he has a specific attacking strategy targeting every time the most vulnerable and susceptible node; ii) Disorderly attacker: he has no attacking strategy and every time hits randomly a node; iii) No security controls: the organization does not implement any security controls; iv) GTM Security Controls: the organization follows all the GTM suggestions and aims to protect its infrastructure by integrating an approach followed by a Game Theory attacker and v) Randomized Security Controls: follows only the 0-1 Knapsack problem and randomly implements security controls. Furthermore, the following experiments have been performed: i) Game Theory attacker VS No security controls; ii) Game Theory attacker VS GTM Security Controls; iii) Game Theory attacker VS Randomized Security Controls; iv) Disorderly attacker VS No security controls; v) Disorderly attacker VS GTM Security Controls and vi) Disorderly attacker VS Randomized Security Controls. Each experiment was executed 6000 times. The results are presented in Table 2.

Table 2: Single Target

	Game Theory Attacker	Disorderly Attacker
GTM	Total Success: 191 3.19%	Total Success: 156 2.6%
No Sec. Control	Total Success: 756 12.6%	Total Success: 539 8.99%
Randomized	Total Success: 373 6.22%	Total Success: 247 4.65%

On the one hand, GTM decides to protect the following paths: BE, EF, and DF (see Figure 3). On the other hand, the randomized approach protects all nodes apart from path BE. In this case study, GTM and the randomized approach spent the whole budget (100%). GTM combining the game-theoretic approach and the 0-1 Knapsack problem mitigates the cybersecurity risk more than the other approaches. Overall, the GTM protected fewer paths than the randomized approach achieving a higher level of security.

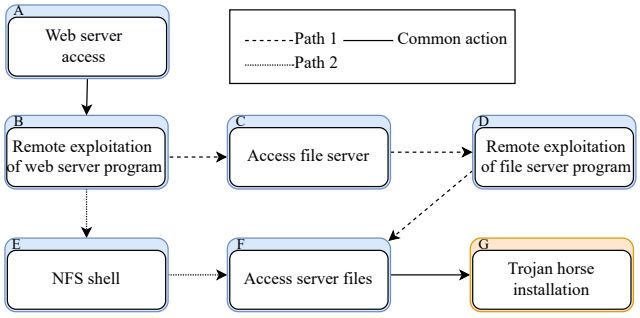

Figure 3: Single Target

4.2 Attacker with multiple targets

In this case study, the results of networking scanning and penetration testing of an e-shop have been utilized for the attack graph generation. The aforementioned data was provided voluntarily by a colleague who serves as CISO in this specific e-shop. The Attacker

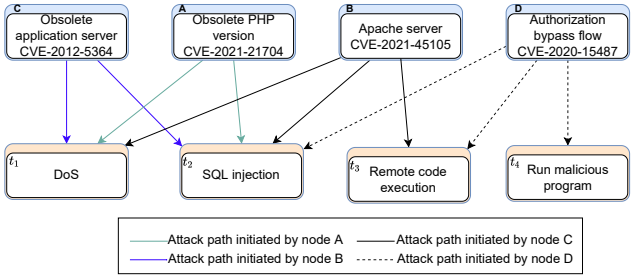

Figure 4: Multiple Targets

aims to achieve DoS or SQL injection or remote code execution or install and run a malicious program to the Apache server (see Figure 4). The budget is set at 100 monetary units. The CISO informed us that the impact of a DoS costs 370 monetary units, the impact of SQL injection costs 490 monetary units, the remote code execution costs 550 monetary units and the execution of a malicious program is 440 monetary units. The probability of an attack to be successfully executed has been defined as follows, $P_{(A,t_1)} = 0.16$, $P_{(A,t_2)} = 0.24$, $P_{(B,t_1)} = 0.8$, $P_{(B,t_2)} = 0.7$, $P_{(B,t_4)} = 0.7$, $P_{(C,t_1)} = 0.6$, $P_{(C,t_2)} = 0.36$, $P_{(D,t_2)} = 0.54$ $P_{(D,t_3)} = 0.2$ and $P_{(D,t_4)} = 0.16$ (see Figure 4); the aforementioned are arbitrary values provided by the CISO based on his experience. Also, the following participants have been defined: i) Game Theory attacker: he has a specific attacking strategy targeting every time the most vulnerable and susceptible node; ii) Disorderly attacker: he has no attacking strategy and every time hits randomly a node; iii) No security controls: the organization does not implement any security controls; iv) GTM Security Controls: the organization follows all the GTM suggestions and aims to protect its infrastructure by integrating an approach followed by a Game Theory attacker and v) Randomized Security Controls: follows only the 0-1 Knapsack problem and randomly implements security controls. Furthermore, the following experiments have been performed: i) Game Theory attacker VS No security controls; ii) Game Theory attacker VS GTM Security Controls; iii) Game Theory attacker VS Randomized Security Controls; iv) Disorderly attacker VS No security controls; v) Disorderly attacker VS GTM Security Controls and vi) Disorderly attacker VS Randomized Security Controls. Each experiment was executed 6000 times. The results are presented in Table 3.

On the one hand, GTM decided to protect the paths generated by the attacking source (node) B spending 85% of the budget. On the other hand, the randomized approach protected the paths generated by attacking source A, C, and D spending the whole budget. One can observe that GTM provides the best strategy for the mitigation of the cybersecurity risk, namely, it decreases the cybersecurity risk more than the other approaches. In summary, GTM spent less part of the budget than other approaches to achieving a better security level.

4.3 Technical, physical and environmental vulnerabilities

It is known that the real cost that is spent for cybersecurity is not limited to the technical vulnerabilities (e.g., CVEs) but it includes

Table 3: Multiple Targets

	Game Theory Attacker	Disorderly Attacker
GTM (cost 85)	Total Success: 1,500 25%	Total Success: 1,444 24%
No Sec. Control	Total Success: 2,977 49.6%	Total Success: 2,689 44.8%
Randomized (cost 100)	Total Success: 1,782 29.7%	Total Success: 1,384 23%

also physical and environmental vulnerabilities [18]. The CISO of the aforementioned e-shop, informed us that the security budget will not be allocated only in CVE patching processes (because in the majority of cases the CVE-patching is completed through updates and is part of indirect costs), but in activities including but not limited to increasing the awareness of the employees, equipment protection, and operational security (e.g., CRM, ERP). This can be verified by the ISO 27001:2013 [14] that obligates prominent certified organizations to meet specific security requirements, e.g., phishing campaigns against the employees per year, implementation of CCTV, and access control mechanisms in the organization's infrastructure. The CISO provided us with the risk assessment report that is depicted in Table 4. The report contains the threats and vulnerabilities that an attacker can exploit, the probabilities of occurrence and exploitation, as well as the impact values describing the organization's damage in monetary units in case of occurrence of each threat. The probabilities have been estimated in qualitative values ($\underline{M}$:Medium - $\underline{L}$:Low - $\underline{H}$:High). Also, the threats that are incorporated in this use-case have been qualitatively predicted ($\underline{L}$: Low occurrence -$\underline{M}$: Medium occurrence - $\underline{H}$: High occurrence) instead of quantitatively. Furthermore, there is a match between threats and controls, together with the efficacy and the cost of the control. However, this case study is not a game between an Attacker and a Defender, since the SME has to defend against numerous threats instead of a single adversary aiming to compromise an organization, which is independent without interconnections among them.

In this case study, the CISO has to handle a budget that has been set at 100 monetary units. At this point, the GTM via the 0-1 Knapsack algorithm, a pillar of the proposed methodology, chooses to implement the replacement of the IT administrator and install fire detectors spending 95% of the budget. These situations cannot be modeled using game theory due to its incapability to handle complex factors and situations.

5 CONCLUSION

This paper introduces a methodology developed as a software tool has been presented, named GTM. GTM proposes game-theoretic investment strategies against different types of attackers (namely, game-theoretic and disorderly) and is applicable to various scenarios with one or multiple attacking targets. The evaluation of GTM concluded that the beneficiaries are able automatically to create defensive strategies that can effectively operate in various scenarios.

At the core of GTM lies the Game Theory approach based on Nash equilibrium, which when combined with a manual input, regarding the occurrence and exploitation probabilities, from the user (CISO) it can predict an attacker's behavior. As the number of

Table 4: Risk assessment report

Threat (i)	Vulnerability	R_i	P_i	Impact	Control	Control Efficacy	Control Cost
Compromised server	No PenTests	M	M	100000	PenTest	0.8	50
Unauthorized network access	No PenTest	M	M	15000	PenTest	0.9	
No replacement for IT admin	SPoF	H	L	250000	Hire replacement	0.9	85
No replacement for IT admin	SPoF	H	L	250000	Outsource the duties	0.7	70
Air condition failure	No generator/UPS	H	M	30000	Provision of generator/UPS	0.9	20
Compromised DB	Obsolete OS	H	M	30000	Server Mitigation	0.8	35
Compromised DB	Obsolete OS	H	M	30000	Move to isolated network zone	0.3	10
Malware infection	No endpoint AV and admin rights to developer PCs	M	M	100000	AV	0.9	25
Fire in the server room	No fire detectors	M	L	100000	fire detectors installation	0.7	10
Data exfiltration	No DLP	H	M	40000	DLP provision	0.9	25
SQLi	CVE-2021-44832	H	H	15000	Security Updates	0.7	
DoS	CVE-2021-44832	H	H	12000	Security Updates	0.7	20
RCE	CVE-2021-44832	M	H	20000	Security Updates	0.7	
Unauthorized entry	No access control	H	M	15000	Access Control	0.8	35

security incidents and challenges is rising, more security vulnerabilities are emerging, creating a fertile surface for adversaries to exploit them for their benefit. GTM can facilitate CISOs' by providing smart defensive strategies which have as main goal to achieve the maximum security level with the minimum budget. The budget is optimally allocated to the nodes that play a key role in a cyber attack.

The outcomes of this paper can be used as the basis for future work in a variety of ways. Particularly, GTM has been developed as a prototype for Linux-based environments for the presented proof-of-concept implementation. Next, we plan to implement the GTM for Windows-based environments removing environment-related barriers, as well as we aim to calculate the return of investment of each node and their interdependencies. Consequently, we intend to integrate the Best-First search algorithm to select the path that is most profitable. We aim to develop an Ant Colony Optimization algorithm populating the most significant system vulnerabilities. Finally, future work will focus on the GTM's assessment against an attack graph that represents an LE that handles a complex scenario including numerous attackers and numerous targets in one game.

ACKNOWLEDGMENTS

This research has been funded by the European Commission (Horizon 2020 Programme), and particularly by the projects SECONDO (Grant Agreement no. 823997) and CyberSec4Europe (Grant Agreement no. 830929) as well as by Operational Programme Competitiveness, Entrepreneurship and Innovation 2014-2020 (EPAnEK), under the project NetPHISH (Grant Agreement no. T1EΔK-05112).

REFERENCES

[1] Mustafa Abdallah, Parinaz Naghizadeh, Ashish R Hota, Timothy Cason, Saurabh Bagchi, and Shreyas Sundaram. 2020. Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs. *IEEE Transactions on Control of Network Systems* 7, 4 (2020), 1585–1596.

[2] Mohamed G Ahmed, Sakshyam Panda, Christos Xenakis, and Emmanouil Panaousis. 2022. MITRE ATT&CK-driven Cyber Risk Assessment. In *The 17th International Conference on Availability, Reliability and Security*.

[3] Nadia Boumkheld, Sakshyam Panda, Stefan Rass, and Emmanouil Panaousis. 2019. Honeypot Type Selection Games for Smart Grid Networks. In *Decision and Game Theory for Security*, Tansu Alpcan, Yevgeniy Vorobeychik, John S. Baras, and György Dán (Eds.). Springer International Publishing, Cham, 85–96.

[4] Panagiotis Bountakas, Konstantinos Koutroumpouchos, and Christos Xenakis. 2021. A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection. In *The 16th International Conference on Availability, Reliability and Security* (Vienna, Austria) *(ARES 2021)*. Association for Computing Machinery, New York, NY, USA, Article 127, 12 pages. https://doi.org/10.1145/3465481.3469205

[5] Panagiotis Bountakas, Christoforos Ntantogian, and Christos Xenakis. 2022. EKnad: Exploit Kits' network activity detection. *Future Generation Computer Systems* 134 (2022), 219–235. https://doi.org/10.1016/j.future.2022.04.001

[6] Renew Europe. 2021. Internet Security Report - Q3 2021. https://www.watchguard.com/wgrd-resource-center/security-report-q3-2021. [Online; accessed 19-April-2022].

[7] Renew Europe. 2021. SMEs in the European Data-Economy. https://www.reneweuropegroup.eu/campaigns/2021-07-01/europes-small-and-medium-sized-enterprises-start-ups-and-entrepreneurs-are-a-renew-europe-priority. [Online; accessed 19-April-2022].

[8] Renew Europe. 2022. 25+ cyber security vulnerability statistics and facts of 2021. https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/. [Online; accessed 19-April-2022].

[9] Zexuan Fan and Xiaolong Xu. 2019. APDPk-means: A new differential privacy clustering algorithm based on arithmetic progression privacy budget allocation. In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 1737–1742.

[10] Aristeidis Farao, Sakshyam Panda, Sofia Anna Menesidou, Entso Veliou, Nikolaos Episkopos, George Kalatzantonakis, Farnaz Mohammadi, Nikolaos Georgopoulos, Michael Sirivianos, Nikos Salamanos, Spyros Loizou, Michalis Pingos, John Polley, Andrew Fielder, Emmanouil Panaousis, and Christos Xenakis. 2020. SECONDO: A Platform for Cybersecurity Investments and Cyber Insurance Decisions. In *Trust, Privacy and Security in Digital Business*, Stefanos Gritzalis, Edgar R. Weippl, Gabriele Kotsis, A. Min Tjoa, and Ismail Khalil (Eds.). Springer International Publishing, Cham, 65–74.

[11] Aristeidis Farao, Eleni Veroni, Christoforos Ntantogian, and Christos Xenakis. 2021. P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go. *Sensors* 21, 8 (2021), 2686.

[12] Andrew Fielder, Emmanouil Panaousis, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. 2016. Decision support approaches for cyber security investment. *Decision support systems* 86 (2016), 13–23.

[13] FIRST. 2022. Common Vulnerability Scoring System SIG. https://www.first.org/cvss/. [Online; accessed 19-April-2022].

[14] ISO. 2013. ISO/IEC 27001:2013. https://www.iso.org/standard/54534.html. [Online; accessed 19-April-2022].

[15] Igor Kotenko and Elena Doynikova. 2014. Security assessment of computer networks based on attack graphs and security events. In *Information and Communication Technology-EurAsia Conference*. Springer, 462–471.

[16] P Mishra and Garima Tyagi. 2018. Game theory based attack graph analysis for Cyber war strategy. *INDIACom* (2018).

[17] Antonio Muñoz, Aristeidis Farao, Jordy Ryan Casas Correia, and Christos Xenakis. 2020. ICITPM: integrity validation of software in iterative continuous integration through the use of Trusted Platform Module (TPM). In *European Symposium on Research in Computer Security*. Springer, 147–165.

[18] Antonio Muñoz, Aristeidis Farao, Jordy Ryan Casas Correia, and Christos Xenakis. 2021. P2ISE: Preserving Project Integrity in CI/CD Based on Secure Elements. *Information* 12, 9 (2021), 357.

[19] NIST. 2007. Information security handbook: A guide for managers, NIST special publication 800-100.

[20] NIST. 2012. Nist. guide for conducting risk assessment, NIST special publication 800-30 revision 1.

[21] Christoforos Ntantogian, Panagiotis Bountakas, Dimitris Antonaropoulos, Constantinos Patsakis, and Christos Xenakis. 2021. NodeXP: NOde. js server-side JavaScript injection vulnerability DEtection and eXPloitation. *Journal of Information Security and Applications* 58 (2021), 102752.

[22] Xinming Ou, Sudhakar Govindavajhala, Andrew W Appel, et al. 2005. MulVAL: A Logic-based Network Security Analyzer.. In *USENIX security symposium*, Vol. 8.

USENIX security symposium, Baltimore, MD, 113–128.

[23] Emmanouil Panaousis, Andrew Fielder, Pasquale Malacaria, Chris Hankin, and Fabrizio Smeraldi. 2014. Cybersecurity games and investments: A decision support approach. In *International Conference on Decision and Game Theory for Security*. Springer, Springer, Cham, 266–286.

[24] Sakshyam Panda, Aristeidis Farao, Emmanouil Panaousis, and Christos Xenakis. 2019. *Cyber-Insurance: Past, Present and Future*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1–4. https://doi.org/10.1007/978-3-642-27739-9_1624-1

[25] S Panda, I Oliver, and S Holtmanns. 2018. Behavioural modelling of attackers' choices. In *Safety and Reliability–Safe Societies in a Changing World*. CRC Press, Boca Raton, Florida, 119–126.

[26] Sakshyam Panda, Emmanouil Panaousis, George Loukas, and Christos Laoudias. 2020. Optimizing investments in cyber hygiene for protecting healthcare users. In *From Lambda Calculus to Cybersecurity Through Program Analysis*. Springer, Cham, 268–291.

[27] Sakshyam Panda, Stefan Rass, Sotiris Moschoyiannis, Kaitai Liang, George Loukas, and Emmanouil Panaousis. 2021. HoneyCar: A Framework to Configure Honeypot Vulnerabilities on the Internet of Vehicles. https://doi.org/10.48550/ARXIV.2111.02364

[28] Sakshyam Panda, Daniel W Woods, Aron Laszka, Andrew Fielder, and Emmanouil Panaousis. 2019. Post-incident audits on cyber insurance discounts. *Computers & Security* 87 (2019), 101593.

[29] Nikolaos Polatidis, Elias Pimenidis, Michalis Pavlidis, Spyridon Papastergiou, and Haralambos Mouratidis. 2020. From product recommendation to cyber-attack prediction: Generating attack graphs and predicting future attacks. *Evolving Systems* 11, 3 (2020), 479–490.

[30] Emma Scott, Sakshyam Panda, George Loukas, and Emmanouil Panaousis. 2022. Optimising User Security Recommendations for AI-powered Smart-homes. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, IEEE, New York, NY, USA, 921–937.

[31] Anoop Singhal and Xinming Ou. 2017. Security risk analysis of enterprise networks using probabilistic attack graphs. In *Network Security Metrics*. Springer, Cham, 53–73.

[32] Orly Stan, Ron Bitton, Michal Ezrets, Moran Dadon, Masaki Inokuchi, Ohta Yoshinobu, Yagyu Tomohiko, Yuval Elovici, and Asaf Shabtai. 2020. Extending attack graphs to represent cyber-attacks in communication protocols and modern it networks. *IEEE Transactions on Dependable and Secure Computing* 19 (2020), 1936–1954.

[33] Branka Stojanović, Katharina Hofer-Schmitz, and Ulrike Kleb. 2020. APT datasets and attack modeling for automated detection methods: A review. *Computers & Security* 92 (2020), 101734.

[34] George Suciu, Cristiana-Ioana Istrate, Alexandru Vulpe, Mari-Anais Sachian, Marius Vochin, Aristeidis Farao, and Christos Xenakis. 2019. Attribute-based access control for secure and resilient smart grids. In *6th International Symposium for ICS & SCADA Cyber Security Research 2019 6*. ScienceOpen, Inc., 155 Middlesex Turnpike Burlington, MA 01803 USA, 67–73.

[35] Carol Taylor, Axel Krings, and Jim Alves-Foss. 2002. Risk analysis and probabilistic survivability assessment (RAPSA): An assessment approach for power substation hardening. In *Proc. ACM Workshop on Scientific Aspects of Cyber Terrorism,(SACT), Washington DC*, Vol. 64. Association for Computing Machinery, New York, NY, USA.

[36] Tenable. 2022. Nessus: Network vulnerability scanning tool. https://www.tenable.com/products/nessus. [Online; accessed 14-April-2022].

[37] Shuzhen Wang, Zonghua Zhang, and Youki Kadobayashi. 2013. Exploring attack graph for cost-benefit security hardening: A probabilistic approach. *Computers & security* 32 (2013), 158–169.

[38] Shaun S Wang. 2019. Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal* 57 (2019), 101173.

[39] Michael E Whitman and Herbert J Mattord. 2013. *Management of information security*. Cengage Learning, 20 Channel Center Street Boston, MA 02110 USA.

[40] Shengwei Yi, Yong Peng, Qi Xiong, Ting Wang, Zhonghua Dai, Haihui Gao, Junfeng Xu, Jiteng Wang, and Lijuan Xu. 2013. Overview on attack graph generation and visualization technology. In *2013 International Conference on Anti-Counterfeiting, Security and Identification (ASID)*. IEEE, IEEE, New York, NY, USA, 1–6.