Evaluation of complex security scenarios using defense trees and economic indexes

Article *in* Journal of Experimental & Theoretical Artificial Intelligence · January 2011

DOI: 10.1080/13623079.2011.587206

CITATIONS
19

READS
2,392

4 authors, including:

Stefano Bistarelli
Università degli Studi di Perugia
284 PUBLICATIONS **4,047** CITATIONS
SEE PROFILE

Fabio Fioravanti
Università degli Studi G. d'Annunzio Chieti e Pescara
89 PUBLICATIONS **867** CITATIONS
SEE PROFILE

Francesco Santini
Università degli Studi di Perugia
138 PUBLICATIONS **1,013** CITATIONS
SEE PROFILE

Journal of Experimental & Theoretical Artificial Intelligence
Vol. 00, No. 00, Month-Month 200x, 1–22

Evaluation of complex security scenarios using defense trees and economic indexes[†]

Stefano Bistarelli
Università di Perugia, Email: bista@dmi.unipg.it
Fabio Fioravanti
Università "G. d'Annunzio", Pescara, Italy, Email: fioravanti@sci.unich.it,
Pamela Peretti
Università "G. d'Annunzio", Pescara, Italy, Email: peretti@sci.unich.it,
Francesco Santini*
Università di Perugia, Email: francesco.santini@dmi.unipg.it
(*July 2010*)

In this paper we present a mixed qualitative and quantitative approach for evaluation of Information Technology (IT) security investments. For this purpose, we model security scenarios by using *defense trees*, an extension of attack trees with countermeasures and we use economic quantitative indexes for computing the defender's return on security investment and the attacker's return on attack. We show how our approach can be used to evaluate economic profitability of countermeasures and their deterrent effect on attackers, thus providing decision makers with a useful tool for performing better evaluation of IT security investments during the risk management process.

Keywords: Security scenarios, defense tree, economic indexes, ROI, ROA.

1 Introduction

Security has become today a fundamental part of the enterprise investment in information technology. In fact, more and more cases are reported showing the importance of assuring an adequate level of protection to the enterprise's assets.

In order to focus the real and concrete threat that could affect the enterprise's assets, a risk management process is needed in order to identify, describe and analyze the possible vulnerabilities that must be eliminated or reduced. The final goal of this process is to make security managers aware of the possible risks, and to guide them toward the adoption of a set of countermeasures which can bring the overall risk under an acceptable level.

The determination of the acceptable risk level and the selection of the best countermeasure is unfortunately not an easy duty. There are few methodologies in literature for the process (see Section 2), and often security managers have to decide among too many alternatives. Usually, two possible approaches for the security risk management process can be followed: the qualitative and the quantitative ones. The qualitative approach is based on comparative evaluation of risks, whilst the quantitative approach tries to give precise and objective measures of risk.

In this paper we define a methodology to combine the benefits of the two approaches. The qualitative approach will be used to model security scenarios (via a modified version of attack trees [34, 2, 35, 27]),

[†]Research partially supported by the MIUR PRIN 20089M932N: "Innovative and multi-disciplinary approaches for constraint and preference reasoning, by CCOS FLOSS project "Software open source per la gestione dell'epigrafia dei corpus di lingue antiche", and by INDAM GNCS project "Fairness, Equità e Linguaggi".
*Corresponding author

Journal of Experimental & Theoretical Artificial Intelligence
ISSN 0952-813X print/ ISSN 1362-3079 online ©2006 Taylor & Francis Ltd
http://www.tandf.co.uk/journals
DOI: 10.1080/09528130xxxxxxxxxxxx

and quantitative indexes [20, 21] will be used to measure risk. More in detail, we define *defense trees* by extending attacks trees with countermeasures. We label each node representing a specified vulnerability with a set of countermeasures which mitigate the damage of threats leveraging such a vulnerability. Then we introduce economic indexes associated to the countermeasures. The *Return on Investment* (ROI) [38, 36] index gives a measure of the efficacy of a specific security investment in a countermeasure w.r.t. a specific attack. The *Return on Attack* (ROA) [10] is instead an index that is aimed at measuring the convenience of attacks, by considering the impact of a security solution on attacker's behavior.

Notice that some parameters in the following dissertation, as the annual rate of occurrence (ARO) of attacks, can be difficult to estimate, because organizations are typically reluctant to make attack data publicly available due to the negative influence this may have on their reputation.

We had not the goal to propose a methodology to assess risk and identify the resources to protect. There are many studies [17] that describe the best methodology for this phase of the risk assessment. In this paper we want to describe instead a decision support methodology that could be useful whenever a quantification and detection of the risks and threats have been (someway) performed.

The paper has the following structure. In Section 2 we show the main related work and, in Section 3 we describe the security risk management process. In particular, in Section 3.1 a qualitative approach to scenario analysis based on attack trees is exemplified, and in Section 3.2 we introduce the quantitative indexes ROI and ROA. In Section 4 we define defense trees as an extension with countermeasures of classical attack trees and in Section 5 defense trees are enriched with economic indicators. In Section 6 ROI and ROA are extended to evaluate complex scenarios with multiple attacks and multiple countermeasures. Some approaches to compose the two indexes is provided in Section 7 and the related tables are shown in Appendix B. inally, Section 8 summarizes the paper and sketches some directions for future work.

2 Related Work

In this section we discuss some works related to the approach of our paper. Common instruments used to perform a qualitative analysis of the problem are attack trees. *Attack trees* [34, 35] can be used as a tool to easily provide a visual representation of an attack scenario to facilitate the process of security threat modeling. The root of an attack tree is a specific attack goal, that is progressively decomposed into more detailed sub-goals (a more detailed description of attack trees was presented in Section 3.1). An important characteristic of attack trees is the ability to reuse the tree. Moore *et al.* in [27] proposed the use of *attack pattern* a generic representation of a deliberate, malicious attack that commonly occurs in specific contexts. Each attack pattern contains: the overall goal of the attack specified by the pattern, a list of *preconditions* for its use, the steps for carrying out the attack, and finally a list of *postconditions* that are true if the attack is successful. One may also see examples of the use of direct acyclic graphs to model security scenarios in both Foster's thesis and Schechter's thesis [13, 33], both of which include discussions and histories of the evolution of these structures (fault tree [39], event tree [30], attack tree [34, 35] and attack net [25]).

Other examples of tree structure are then presented by Caelli *et al.* [7] in the 90's, they integrate safeguards into direct acyclic graph by representing them as nodes, placed throughout the diagram. Even in the popular Microsoft text by Howard and LeBlanc, "Writing Secure Code", one can find threat trees in which countermeasures are integrated [18].

A different approach is proposed by Gordon and Loeb in [16] where the authors presents an economic model for determining the optimal security investment for protecting a system from a single threat. They consider three parameters: the monetary loss produced by an occurring breach (λ), the probability of a threat (t), and the probability that an attack would be successful (v) (that correspond respectively to our SLE, ARO and $(1 - RM)$). The expected benefit of an IT investment is modeled as a function of the security investment ($EBIS(z)$). By assuming that "as the investment in security increases, the information is made more secure, but at a decreasing rate", the optimal amount of investment is determined by maximizing the relative difference between benefits and costs.

The Gordon-Loeb model also shows that, for a given level of potential loss, the optimal amount to spend to protect an information set does not always increase with increases in the information set's vulnerabil-

ity. In other words, organizations may drive a higher return on their security activities by investing in cyber/information security activities that are direct at improving the security of information sets with a medium level of vulnerability.

The interconnections and complexity of the economy can have a huge effect on the destructiveness of cyberattacks. There is a limited understanding of how to quantify the consequence of an attack because combinations of cyberattacks could be much more destructive than individual attacks. In [6] are analyzed three features that can influence the complexity of the attacker's behavior: *redundancies*, *interdependencies* and *monopolies*.

Economic redundancies: systems can be simply substitute with other systems by performing similar functions. To deal with redundancies attackers need to employ combinations of cyberattacks designed to produce intensifier effects. These are simultaneous attacks on different systems or business that could otherwise serve as substitutes for each other.

Economic interdependencies: the production in our economy is organized into value-chain, products passes through a series of production phases and at each activity the product gains some value. All these phases can be put in place in separate companies generation many interdependencies among different business. These interconnections generate a big opportunity for attackers that can try to exploit value-chain interdependencies in order to produce a cascade attack.

Economic near monopolies: is a situation in which one or two companies provide the same essential product or service to an entire industry. In this case an attacker can attack the business operations that already leverage a facilitating capability same essential product or service to an entire industry to offer large or widespread benefits with limited means. In this way he can produce a massive damage.

In [8] was described a methodology for quantitatively optimizing the blend of architectural and policy recommendations that engineers can apply to their products to maximize security under a fixed budget. They first analyze *misuse cases* (similar to our attack scenarios) in order to quantify their impact and determine the possible recommendations. Then they prioritize recommendation implementation assigning a cost to each one in order to estimate the total yearly cost. In their approach they also consider if some misuse is unresolved in such way that they can determine also the expected total yearly loss.

[29] is also an interesting lecture, giving pointer to several survey about security attacks and protection. The paper also highlights the different technologies used in the different surveys and the different instruments used to conduit the surveys. This show the difficulty to collect data on this topic. Researchers are proposing new metrics to address cost assignment challenges. For example, Fariborz Farahmand and his colleagues consider using damage assessment across predefined categories as an evaluative framework [12] Schechter introduces cost-to-break (that is, the effort required to invade a system) as a measure of security strength [32] Cost-to-break and security strength work together to help model the effort an attacker must expend to gain access to a system.

Also [1] deal with the problem of data collection and of the absence of a uniform methodology to compute the real risk of each security attack. In particular in [1] the idea of cyberinsurance is considered and many are the prospective benefits suggested by the authors like the introduction of better quantitative tools and metrics for assessing security, the data aggregation and the promulgation of best practices.

Another economic-based framework is proposed in [23] where a game-theoretic approach is used for inferring the attacker's intents, objectives and strategies which are modeled using economic incentives and utilities.

3 Security risk management

The Risk Management process is a fundamental activity in an enterprise since it allows senior managers to make good decisions, thus protecting the organization and its ability to achieve its mission. Many risks can affect an organization's resources: risks related to the political and social environment where the organization works (*strategic risks*); risks related to the money market and interest rate (*financial risks*), and risks related to its business processes (*operative risks*).

In this paper we pay attention to the *Security Risk Management* process [38], that focuses on protecting an enterprise's assets from the *Information Technology Risk* (as part of the operative risk). The Information

Technology Risk considers interruption of services, diffusion of reserved information or loss of data stored on IT systems. More precisely, the risk function can be defined as follows.

Definition 3.1 [Security Risk [38]]. The *Security Risk* [38] is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization's assets. □

At the beginning of the Security Risk Management process, the different *assets* that compose the IT system are identified and analyzed.

Definition 3.2 [Asset]. An *asset* is any tangible or intangible item owned by an organization that has a value for an enterprise and that needs protection. □

During the risk management process, the following phases are performed for each asset: risk assessment, mitigation and monitoring.

Risk Assessment

The Risk Assessment phase is performed with the goal of identifying risks, determining the possible damages, quantifying the impact of potential threats and providing an economic balance between the economic *impact* of risk and the cost of risk mitigation. The output of the risk assessment phase is a report that describes *threats* and *vulnerabilities* that can harm a system, gives measures about the risk and provides recommendations for the implementation of effective *countermeasures*. Following [19, 38],

- a *threat* is the potential for a threat-source to exercise (by accidental trigger or intentional exploit) a specific vulnerability;
- a *vulnerability* is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (by accidental trigger or intentional exploit) by an attack and result in a security breach or a violation of the system's security policy;
- the *impact* is the magnitude of harm that could be caused by a threat's exercise of a vulnerability;
- a *countermeasure* is a control which should be implemented in order to reduce the ability for an attacker to leverage existing system vulnerabilities.

Risk Mitigation

During the Risk Mitigation phase a systematic methodology is used by senior management to prioritize, evaluate and implement countermeasures recommended by the risk assessment process. Based on the risk level presented in the risk assessment report, the implementation actions are prioritized. Every alternative solution is analyzed and the most appropriate and cost-effective ones are selected for actual implementation.

Monitoring

The Monitoring phase is the last phase of the risk management process. During this phase the effectiveness of the implemented countermeasures is evaluated.

In this paper we pay attention on the security risk assessment phase where the security officer has to identify the possible attacks to a system and has to provide recommendations for the implementation of countermeasures able to stop or reduce the possible damage produced by an attack. Generally the techniques used during this phase can be classified in *qualitative* and *quantitative* approaches.

3.1 *The qualitative approaches*

The *qualitative approach* [14] evaluates the security risk level of an IT system by using a variety of polling, interview, and questionnaire techniques with the aim of comparatively ranking assets and threats according to their perceived criticality and likelihood, respectively. A *scenario analysis* is usually adopted, which requires the construction of different scenarios of computer security compromise, in order to illustrate how vulnerable an organization is to information technology attacks [37].

A particular kind of instruments that can be used to conduct a scenario analysis are *attack trees* [34, 35]. Attack trees, AT, provide a formal and methodical way of describing how attacks against a system can be performed.

An attack scenario can be represented in a tree-based structure whose root represents the attacker's final

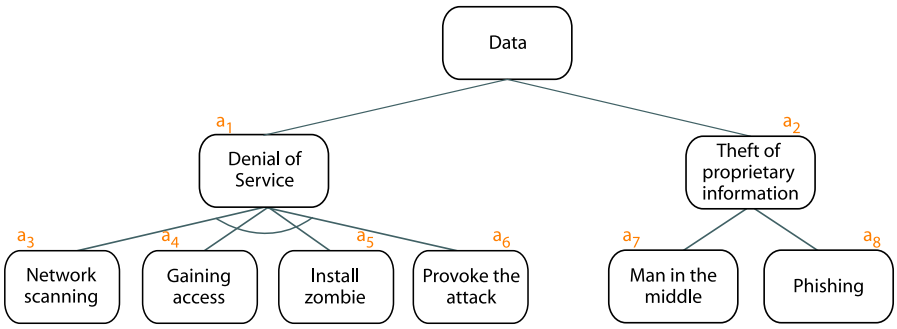

Figure 1. An example attack tree.

goal and paths from leaf nodes to the root represent the different ways of achieving this goal. The root of the tree is associated with an asset of the IT system under consideration. Leaf nodes represent simple subgoals which lead the attacker to (partially) damage the asset by exploiting a single vulnerability. Non-leaf nodes (including the tree root) represent attack subgoals and can be of two different types: `or`-nodes and `and`-nodes. Subgoals associated with `or`-nodes can be achieved by achieving any of its child nodes, whilst `and`-nodes represent subgoals which can only be achieved by achieving all its child nodes.

Summarizing the attack tree are used to represent attack *actions* and *strategies*: an *attack action* can be defined as a single step that an attacker has to perform to achieve a subgoal, it can be represented by using an `and/or`-node of the attack tree; an *attack strategy*, instead, is a set of attack actions such that all of them are the leaves of one of the possible `and`-tree deriving from an attack tree.

For example, we can associate the tree root with an asset of a system (like, for example, computers, databases, information, etc.) and represent in a tree all the different alternative attack actions that an attacker must perform to successfully attack the system. Remember that each attack action can be represented by using an `and/or`-node: we distinguish the type of a node by drawing a line over the arcs connecting an `and`-node to its children, in order to differentiate it from an `or`-node. Then each path from leaf nodes to the root ending in an achieved subgoal represents a different attack strategy in the considered scenario.

Below we provide an example of how attack trees can be used to model an attack scenario and to identify which vulnerabilities can be exploited in order to harm a system.

Example 3.3 Consider, as an example, an internet services company offering an hosting service. We can use attack trees to model two different attack scenarios for this asset, by considering: 1) how a malicious person can damage the business activity of the company, or 2) how he can access data about customers. In order to damage the business activity of the company an attacker can perform a Denial of Service attack (DoS) by performing all the following attack actions: *i)* scanning the network to discover some vulnerabilities (a_3), *ii)* gaining access on a machine (a_4), *iii)* installing a zombie (a_5), *iv)* performing the attack activating the zombie (a_6). In order to access data about customers an attacker can follow different alternative attack actions: *i)* performing a man-in-the-middle attack (a_7), *ii)* performing a phishing attack (a_8).

Notice that the DoS attack is an `and`-attack because, in order to successfully perform this attack strategy, the attacker must perform all the actions composing the attack.

3.2 *The quantitative approaches*

The *quantitative approach* [26] assigns absolute numeric attribute values to assets, threats, vulnerabilities and countermeasures. The exact identification of risk and the cost/benefit justification of countermeasures are fundamental for constructing a good risk mitigation strategy.

Within this approach several indexes can be used to estimate the effectiveness of an IT security investment.

Definition 3.4 [Single Loss Exposure [21]]. The *Single Loss Exposure* (SLE) [21] represents a measure

of an organization's loss from a single threat and can be computed by using the following formula:

$$SLE = AV \times EF \tag{1}$$

where, the *Asset Value* (AV) is a synthetic measure of the cost of creation, development, support, replacement and ownership values of an asset, and the *Exposure Factor* (EF) represents a measure of the magnitude of loss or impact on the value of an asset arising from a threat event, and is expressed as a percentage of the asset value. □

Since not all threat events are equally likely to succeed the SLE value can be modified by considering the frequency of the given threat event. This leads us to the following definition.

Definition 3.5 [Annualized Loss Expectancy [21]]. The *Annualized Loss Expectancy* (ALE) [21] is the annually expected financial loss of an organization which can be ascribed to a threat and can be computed by using the following formula:

$$ALE = SLE \times ARO \tag{2}$$

where the *Annualized Rate of Occurrence* (ARO) is a number that represents the estimated number of annual occurrences of a threat event. □

It is important to notice that the estimation of ARO is usually built upon the likelihood of the event and the number of attackers that can exploit the given vulnerability. For example, a meteorite damaging the data center could be estimated to occur only once every 100,000 years and will have an ARO of 0.00001. In contrast, 100 data entry operators attempting an unauthorized access attempt could be estimated to occur six times a year per operator and will have an ARO of 600.

Summarizing the above indexes, SLE gives a measure of the damage of a single threat; the ARO gives the likelihood of a threat to occur in a year; ALE tries to consider both the likelihood and the damage of each threat.

All of the above indexes do not consider the fact that the organization can try to build some defense for reducing the probability of vulnerability exploitation by attackers (e.g. implementing some firewall filtering), or reducing the damage of an attack (e.g. applying some backup strategies). In the following, we will use two indexes which also consider the presence of countermeasures: the Return on Investment (ROI) and the Return on Attack (ROA).

In economics, the profitability of an investment can be analyzed using an index comparing the *expected benefits* of the investment to its *costs*:

$$\frac{benefits - costs}{costs}.$$

In general, if the value of this index is a positive number then the investment is profitable and economically justified, otherwise, if the value of the index is zero or a negative number, then the investment is regarded as a "bad investment". The same formula can be used to analyze any type of investment and the terms of the formula change according to the specific type of investment.

We use the Return on Investment index for an economic evaluation of an enterprise's expenditure in IT security that consists in the introduction, into a system, of some countermeasures able to mitigate the *risk of information technology*. It can be used to compare alternative investment strategies and to evaluate whether an investment is financially justified.

Definition 3.6 [Return on Investment [36]]. Given an attack a and a countermeasure c which is able to mitigate a, the Return on Investment (ROI) is the benefit that a defender of an IT system expects from the introduction of c into the system over the costs for implementing that countermeasure. The ROI

can be computed by using the following formula[1]:

$$ROI_{ac} = \frac{ALE_a - \big(ALE_a \times (1 - RM_c)\big) - CSI_c}{CSI_c} \tag{3}$$

where ALE_a is the annual loss produced by a, RM_c represents the ability of a countermeasure c in reducing the damage produced by the attack (expressed as a numeric value in $[0, 1]$), $1 - RM_c$ corresponds to the inability of a countermeasure c to impair the attack a and CSI_c is the (annualized) cost of the countermeasure. □

In this case the benefit produced by a countermeasure is given by the reduction of the "expected loss", produced by an attack ($ALE_{before\ c} - ALE_{after\ c} = ALE - (ALE \times (1 - RM))$) it correspond to a "cost savings" or an "avoiding loss", while the cost of the investment is the cost of a countermeasure.

However, although consistent with other corporate investment decisions, ROI is considered by some to be not so appropriate for this kind of analysis. Gordon and Loeb contend that ROI does not reveal the true economic rate of return and leads to the wrong investment objectives [15], in fact they suggest that ROI measures the cost savings or the avoided loss. Cavusoglu, Mishra, and Raghunathan suggest that sometimes ROI is frustrated by the need to assign costs to poorly defined outcomes [9]. Moreover the ROI index alone only provides a partial characterization of IT investments, because it lacks to explicitly consider attackers' interests. Assuming that the organization's loss is equal to the attacker gain is often a gross simplification. Also, the cost of an attack cannot be directly related to the cost of the security measure because different solutions at different costs might be perceived as equally expensive to break from the attacker's viewpoint. We now consider also the Return on Attack index (ROA) proposed in [10], which is aimed at measuring the convenience of attacks considering the impact of a security solution on attacker's behavior.

Definition 3.7 [Return on Attack.] The *Return on Attack* (ROA) is the gain that an attacker expects from a successful attack a over the costs he sustains due to the adoption of a countermeasure c by its target. It can be computed by using the following formula:

$$ROA_{ac} = \frac{GI - (GI \times RM_c) - cost_a}{cost_a} \tag{4}$$

where GI is the expected gain of the attack, $GI \times RM_c$ is the lost profit produced by c and $cost_a$ is the cost associated to an attack strategy a. □

This definition slightly modifies the original ROA formulation proposed by Cremonini *et al.* in [10] and used in [4], for highlighting the ratio between benefits and costs. In this case, the *benefit* produced by an attack is given by the difference between the gain that an attacker can obtain when there are no countermeasure implemented into a system (GI) and the lost profit produced by a countermeasure c ($GI \times RM_c$); $cost_a$ is the cost associated to the attack itself. Moreover the new definition of ROA is symmetric with the definition of ROI. While in the following of the paper we use Def. 3.7 to compute ROA, the original version proposed in [10] is:

Definition 3.8 [Return on Attack as defined in [10].] The *Return on Attack* (ROA) is the gain that an attacker expects from a successful attack over the losses that he sustains due to the adoption of security measure S by his target. Is defined as:

$$ROA = \frac{GI}{cost\ before\ S + loss\ caused\ by\ S}$$

where GI is the expected gain from the successful attack on the specified target.

[1]Or equivalently $ROI = [(ALE \times RM) - CSI]/CSI)$.

As we will show in Section 7, a combined use of ROA and ROI indexes allows us to perform a more complete evaluation of a countermeasure, considering not only its effectiveness and profitability but also the deterrent effect produced on the attacker.

4 Defense trees: adding countermeasures to attack trees

Attack trees can be used as a tool to easily provide a visual representation of an attack scenario, and can be used for scenario evaluation when enriched with attacker's attributes (e.g. attacker's competencies, costs, ...) [34, 35].
Our idea is to use attack trees in order to identify all the possible attack strategies against a system and then enrich this structure with qualitative and quantitative information (e.g. possible countermeasures, their efficacy, their cost etc.), thus providing the security officer with a useful tool for deciding how to protect his IT system.

4.1 *Identify attack strategies*

In order to ease the process of identifying all possible attacks, even in deep defense trees, we introduce an algorithm able to identify all the attack strategies depicted into a tree. The algorithm takes an attack tree as input and produces the set of all the possible attack strategies depicted into the tree (remember that an attack strategy is a set of attack actions such that all the actions are the leaves of one of the possible `and`-tree deriving from an attack tree).

More formally the algorithm takes as input an attack tree AT and returns as output a set of attack strategies $AS = \{s_1, \ldots, s_n\}$.

The algorithm `AttackStrategies` uses two functions:

- $type(x)$: is a function that checks the type of a node, in other words checks if a node x is an `and`-node, an `or`-node or a left of the tree and returns the value AND, OR or $LEAF$;
- $children(x)$: is a function that returns the set of the children of node x in AT.

The algorithm starts initializing the set AS as an empty set, a first set s_1 composed by the root and adding s_1 to the set of solution Sol (lines 1–3); then for each set of nodes s_i contained in Sol it proceeds as follows: if all the nodes $x \in s_i$ are leaves of the tree (line 6), then the algorithm has retrieved an attack strategy so it removes s_i to the set Sol (line 8) and adds it to the set AS (line 7); otherwise it proceed checking the type of x: for all the nodes $x \in s_i$ such that x is an `and`-node, then the set s_i is modified replacing x by all its children nodes (lines 10–12); for all the nodes $x \in s_i$ such that x is an `or`-node, the solution s_i is duplicated once for each child t of x and in each new solution the node x is replaced exactly by one of its children t (lines 14–17) and finally the original solution s_i is removed from the set Sol (line 18). The algorithm stops returning the set of attack strategies AS (line 23), that is all the `and`-tree of the `and/or`-tree.

As an example, a detailed of the use of the algorithm `AttackStrategies` considering the attack tree depicted in Figure 1 is given in Appendix A.

4.2 *Identify defense strategies*

As we have shown in Section 4.1, attack trees are a useful tool to represent attack strategies against a system. However, they do not take into account countermeasures which can be implemented by the defending organization and the costs sustained for such security investments.

For this reason, we enrich standard attack trees by decorating every leaf node with a set of countermeasures. Each countermeasure associated with a leaf node represents a possible risk mitigation of the scenario showing the use of the specific vulnerability. We call such attack trees decorated with countermeasures *defense trees* [4].

Definition 4.1 [Defense Tree]. A *defense Tree* is built by labeling each leaf of a given attack tree using

Algorithm 1 `AttackStrategies`(AT)

$AS \leftarrow \emptyset$
$s_1 = \{root\}$
$Sol \leftarrow s_1$
while $Sol \neq \emptyset$ **do**
  for all $s_i \subseteq Sol$ **do**
    if $\forall\ x \in s_i$ s.t. $type(x) = LEAF$ **then**
      $AS \leftarrow s_i$
      $Sol \leftarrow Sol s_i$
    else
      for all $x \in s_i$ s.t. $type(x) = AND$ **do**
        $s_i \leftarrow s_i \cup children(x) \backslash \{x\}$
      end for
      for all $x \in s_i$ s.t. $type(x) = OR$ **do**
        for all $t \in children(x)$ **do**
          $\overline{s}_t \leftarrow s_i \cup \{t\} \backslash \{x\}$
          $Sol \leftarrow Sol \cup \overline{s}_t$
        end for
        $Sol \leftarrow Sol \backslash s_i$
      end for
    end if
  end for
end while
return AS

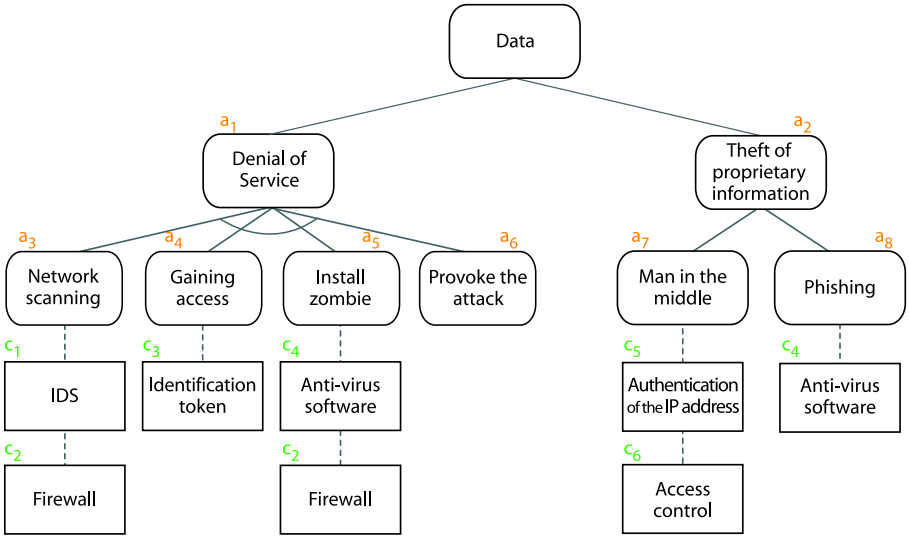

Figure 2. A defense tree for the attack tree of Fig. 1.

those countermeasures which mitigate the attack action on that leaf. □

This new structure helps the security officer to represent in a graphical way the *defense strategies* that a security officer can use. An example defense tree is presented in Fig. 2.

Example 4.2 The attack trees used in Example 3.3 can be enriched with the possible countermeasures that can be introduced to protect the organization's information as follows:
Figure 2 shows some of the countermeasures which can be implemented to reduce the risk of Denial of Service (like, for example, using an intrusion detection system (IDS) or a firewall, using an identification

token or an anti-virus software) and the risk of theft of proprietary information (like, for example, controlling access and authenticating the IP address and using an anti-virus software). An identification token is a small hardware device that the owner carries to authorize access to a network service: for example, the device may be in the form of a smart card.

5 Economic evaluation of threats

In order to obtain a more precise evaluation of attack/defense scenarios we enrich the defense tree modeling the considered scenario by using economic quantitative indexes in order to label the tree with the ROI and ROA. The security officer can use this information to make a more informed decision in the selection of the countermeasures that can be implemented for protecting the system, combining the advantages of attack trees (ease of use, visual modeling of attack scenarios), with the advantages of quantitative approaches (the use of indexes).

Moreover using the decorated defense tree we can analyze the security investment that an organization needs to support considering the scenario from two different points of view: the organization's view and the attacker's view. In particular looking at an attack scenario from the defender's point of view, we can use ROI to determine what countermeasures are cost effective. On the other hand, by using ROA, we can see the same attack scenario from the attacker's point of view and determine the behavior of an attacker, and his favorite attack strategies.

In the following we show, by means of an example, how to label a defense tree with the economic indexes presented in Section 3.2.

5.1 *Computing ROI: the defender's point of view*

Given a defense tree, we describe the defender's point of view by enriching the given tree using economic quantitative labels. In this way, we can determine countermeasures to be selected for implementation taking into account the organization's return on investment. For each asset we want to protect, we proceed as follows: first we estimate the value of the asset, AV, then considering the EF and the ARO associated to each attack we can compute the SLE and the annual loss produced by an attack (ALE). Then we have to consider the RM and the CSI associated to each countermeasure in order to calculate the Return on security Investment associated to each couple attack-countermeasure.

We can use ROI to compare economic profitability of the different countermeasures that an organization can use to protect its own systems. For example, for each attack strategy, we could select the countermeasure which maximizes ROI among all countermeasures which are associated to its vulnerability nodes.

In the following we use (when available) statistics collected in the famous *CSI Computer Crime and Security Survey* [31] and in the *2009 Global Security Survey* [5] two of the most popular publicly available surveys used for this type of analysis.

As an example, consider the defense tree of Figure 2. In the example we consider the asset value of the information stored into a server estimated in 100.000€, and the EF[1] and the ARO[2] of each attack as shown in Tab. 1. In the following example, we consider the CSI cost as already annualized.

Attack strategies		**EF**	**ARO**
s_2	Denial of services	0.07	1
s_4	Man in the middle	0.04	1
s_5	Phishing	0.06	1

Table 1. Exposure Factor (EF) and Annualized Rate of Occurrence (ARO) for the defense tree of Fig. 2.

[1]This value is estimated considering the CSI survey reporting [31] the data of the dollar amount losses by type of attack and the types of attack detected in the 2007. Considering the *financial fraud* as the attack with the highest exposure factor ($EF = 1$), the EF associated to the attacks *Dos*, *Man in the middle* and *Phishing* is respectively 0.07, 0.04 and 0.06 .

[2]We suppose the value of ARO equal to 1 because there are no data available to correctly estimate this information.

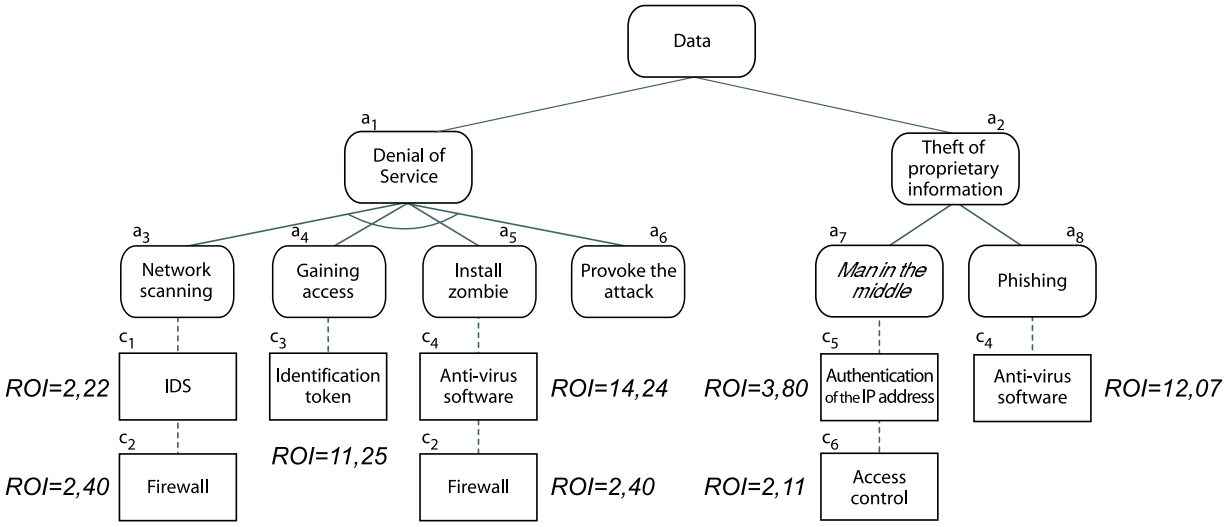

Figure 3. The defense tree of Fig. 2 decorated with ROIs.

Defense strategies		**RM**	**CSI**
c_1	IDS	0.69	1500 €
c_2	Firewall	0.97	2000 €
c_3	Identification token	0.35	200 €
c_4	Anti-virus software	0.98	450 €
c_5	Authentication of the ip address	0.3	250 €
c_6	Access control	0.7	900 €

Table 2. Risk Mitigated (RM) and Cost of Security Investment (CSI) for the defense tree of Fig. 2.

We need now to compute SLE and ALE for each attack strategies. For the first attack, we have

$$SLE = AV \times EF = 100000\,€ \times 0.07 = 7000\,€$$

$$ALE = SLE \times ARO = 7000\,€ \times 1 = 7000\,€.$$

In a similar manner we can compute the value of ALE for the second attack and the third attack: ALE=4000 € and ALE=6000 €, respectively.

As a last step, by considering the countermeasure cost (CSI) and the amount of risk mitigated (RM)[1] associated to each countermeasure and reported in Tab. 2, we can label each countermeasure with the corresponding ROI. For the first countermeasure (installing an IDS), we have

$$ROI = \frac{7000\,€ - \big(7000\,€ \times (1 - 0.69)\big) - 1500\,€}{1500\,€} = 2.22$$

The resulting defense tree showing the value of ROI for each countermeasure is depicted in Figure 3.

From the defense tree of Figure 3 the security manager can already make some considerations. To mitigate all the attacks, at least one countermeasure for each path has to be selected. For each path, the countermeasure with highest ROI is selected (in fact, the higher the ROI the better the investment). So, for the first and the third attack strategies of the example the best countermeasure seems to be the

[1]This value is estimated considering the CSI survey reporting [31] the data of the security technologies used. We can estimate the ability of a countermeasure in mitigate the risk of an attack considering its diffusion.

installation of an anti-virus software with $ROI = 14.24$ and $ROI = 12.07$ respectively. Similarly, for the second attack strategy the best countermeasure is the authentication of the IP address $ROI = 3.80$.

Notice, however, that sometimes a countermeasure can mitigate more than one attack (as is the case for the firewall and the anti-virus software in the defense tree of Figure 2). In this case a more detailed analysis has to be performed, and an overall ROI considering all the attacks and all the countermeasures of the tree has to be computed (see Section 6). Another consideration is about the ROI for a specific countermeasure. From the defense tree of Figure 3 we can see that the same countermeasure (for instance the anti-virus software), can have a different ROI in different attacks ($ROI = 14.24$ and $ROI = 12.07$, respectively). This happens because the level of risk mitigation (RM) of a countermeasure strictly depends from the specific attack, and the ALE of the attacks could be completely different. We discuss solutions to these problems in Section 6.

5.2 *Computing ROA: the attacker's point of view*

Given a defense tree also the attacker's point of view can be considered by using ROA as a countermeasure label. We proceed as follows: first of all we consider for each tree the expected gain deriving from a successful attack (GI) to the the root of the tree; then, we estimate the attack cost to be sustained by an attacker to succeed when no countermeasure is present (Cost) and the effectiveness of the countermeasure to stop the attack (RM); finally, the Return on Attack (ROA) is computed and used as a label for each countermeasure.

Attack strategies		**Cost**
s_2	Denial of services	4000 €
s_4	Man in the middle	2500 €
s_5	Phishing	1000 €

Table 3. Estimated cost of the attacks represented in the defense tree of Fig. 2.

As an example, consider again the defense tree depicted in Figure 2. This time the tree is analyzed from an attacker's perspective. Let us suppose that the attacker has an advantage that can be economically quantified as 30000 € for a successful attack to the server. By using the data of Tables 2 and 3 we can compute the ROA for each countermeasure.

Notice that the cost an attacker has to pay depends on the attack and not on the installed countermeasures. We assume that when the attacker estimates the cost of the attack, he doesn't know exactly what countermeasures have been really implemented.

For instance, when installing an IDS we can obtain

$$ROA = \frac{30000\,€ - (30000\,€ \times 0.69) - 4000\,€}{4000\,€} = 1.33$$

In a similar manner we can compute ROA for all the other countermeasures obtaining the values reported in Figure 4.

Now, the same defense tree can be analyzed by the security manager in a similar manner as already described above for the ROI. This time the lower the ROA the lower the incentive for an attacker to try the specific attack. So, for the first attack strategy of the example the best countermeasure seems to be the installation of an anti-virus software with a $ROA = -0.85$. Similarly, for the second attack strategy the best countermeasure is the use of an access control system with $ROA = 2.60$, and for the last attack strategy the best countermeasure is the use of an anti-virus software with $ROA = -0.40$.

6 Considering multiple attacks and countermeasures

We identify three different and more complex scenarios (Figure 5): the new scenarios we consider extend the original scenario by considering either the case where there can be multiple countermeasures per attack, or multiple attacks per countermeasure, or multiple attacks per multiple countermeasures.

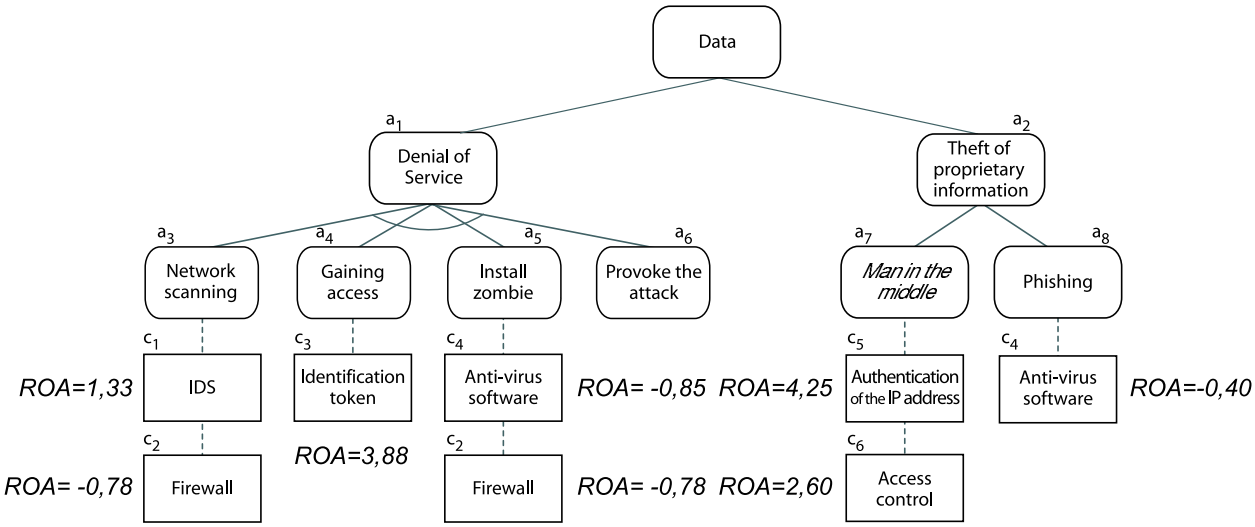

Figure 4. The defense tree of Fig. 2 decorated with ROA.

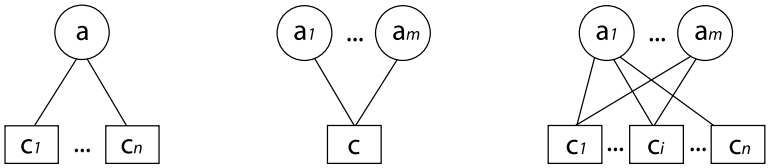

Figure 5. Three different scenarios.

In particular we consider the following scenarios:

(a) a scenario where an attack can be mitigated by using n countermeasures,
(b) a scenario where a single countermeasure can be used to mitigate m attacks,
(c) a more complex scenario where m attacks can be mitigated by using n different countermeasures.

We change the definition of *ROI* and *ROA* to evaluate the profitability and the effectiveness of an investment also in these more general scenarios.

6.1 *Case (a): single attack, multiple countermeasures*

Return on Investment

Sometimes, in order to protect a high value asset, the system administrator may want to deploy more than one countermeasure reducing the loss deriving from an attack (see Figure 5(a)).
In this case it seems reasonable to assume that using multiple countermeasures determines a reduction of the loss produced by the attack itself, for this reason we have to measure what is this reduction analyzing the risk mitigated by a *set* of countermeasures.

Definition 6.1 [Risk Mitigated by a set of countermeasures]. The risk mitigated by a set of countermeasures C used to stop an attack action a, called RM_{aC}, is a function of the risk RM_{ac} associated to each countermeasure $c \in C$ in mitigating the risk produced by the attack a:

$$\max_{c \in C}\{RM_{ac}\} \leq RM_{aC} \leq \min\{1, \sum_{c \in C}(RM_{ac})\}.$$

RM_{ac} is a value between the *maximum* value of the RM_{ac} associated to the countermeasures $c \in C$ and the *sum* of them. □

Remember that the value of RM is a number in $[0, 1]$, and for this reason we assume RM_{aC} as a value between the max RM of the countermeasures that compose the set and the minimum value between 1 and the sum of the RM. Notice that the countermeasures are not additive, but we only fix the lower and the upper bounds of their composition. In particular, in all the examples in this section, we will compute it as $\min\{1, \sum_{c \in C}(RM_{ac})\}$.

In this new scenario where a single attack and multiple countermeasures are considered, the definition of ROI changes as follows:

Definition 6.2 The Return on Investment associated to a set C of n countermeasures able to mitigate the risk associated to an attack strategy a is given by the following formula:

$$ROI_{aC} = \frac{ALE_a - \big(ALE_a \times (1 - RM_{aC})\big) - CSI_C}{CSI_C} \tag{5}$$

where CSI_C is the total cost associated to the set C: $CSI_C = \sum_{c \in C}(CSI_c)$ □

The following example shows how to use this new definition of ROI.

Example 6.3 This example extends the example in Section 5 considering all the possible sets of countermeasures that can be used to protect the system from the attacks strategies s_2, s_4 and s_5.
The set of countermeasures with the highest ROI for the attack strategies s_2, s_4 and s_5 are, respectively, $\{c_4\}$, $\{c_5\}$ and $\{c_4\}$ ($ROI_{(s_2),(c_4)} = 14.24$, $ROI_{(s_4),(c_5)} = 3.80$ and $ROI_{(s_5),(c_4)} = 14.24$). We obtain this result because c_4 and c_5 are cheap countermeasures (they cost respectively 450 € and 250 €) and so they result a good investment to protect the system. Tables B1, B2 and B3 show the values of ROI associated to all the sets of countermeasures.

Return on Attack

When an attacker evaluates the profitability of an attack strategy he has to consider how many countermeasures have been deployed to mitigate the risks of a single attack. In fact the countermeasures implemented into the system reduce the effectiveness of an attack strategy, and consequently, the gain that the attacker can obtain. So we have to modify the definition of ROA and consider the effects produced by a *set* C of countermeasures. Remember that RM_{aC} is a function of the RM's associated to each countermeasure in mitigating the risk produced by an attack a (see Definition 6.1).

The definition of ROA, when we consider a single attack and a set of countermeasures, changes as follows:

Definition 6.4 The Return on Attack, associated to an attack strategy a when there is a set C of countermeasures able to mitigate a, can be computed by using the following formula:

$$ROA_{aC} = \frac{GI - (GI \times RM_{aC}) - cost_a}{cost_a} \tag{6}$$

where GI is the expected gain of the attack a, RM_{aC} is the risk mitigated by the set C and $cost_a$ is the cost associated to an attack strategy a. □

6.2 *Case (b): multiple attacks, single countermeasure*

Return on Investment

Sometimes we can see that one countermeasure can be used to protect the system from the risk associated to more than one attack (see Figure 5(b)). For instance, consider the defense tree of Figure 2. We can see that the countermeasures "install a firewall" and "use an anti-virus software" appear in multiple branches of the tree.

In order to evaluate this scenario we first have to change the representation of the scenario using a *defense graph*, then we have to change the definition of ROI considering that a single countermeasure can be used to reduce the risk associated to a *set* of attacks.

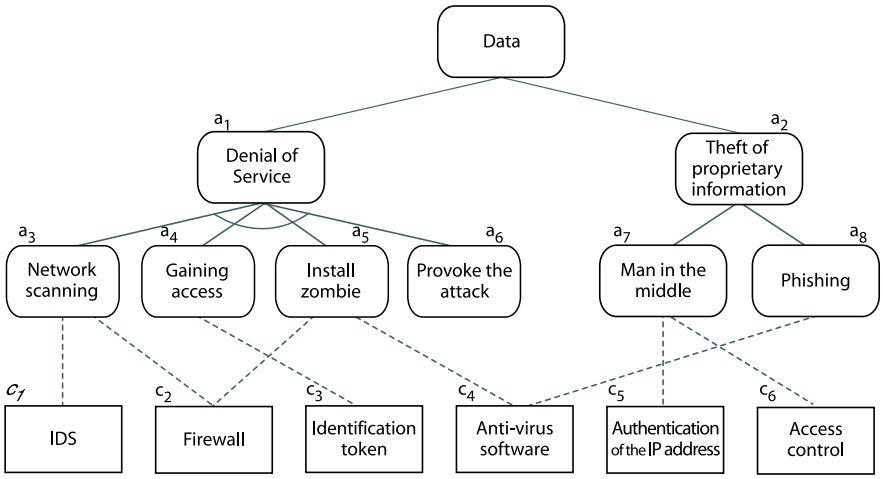

Figure 6. The defense tree of Fig. 2 represented as a defense graph.

Definition 6.5 [Defense graph]. A *defense graph* is a defense tree where each countermeasure is represented once, and can be connected to more than one attack action. □

For instance, the defense tree of Figure 2 can be transformed in the defense graph of Figure 6.
Notice that when we consider a set of possible attacks, we have to measure what are the benefits produced by the use of a defense strategy composed by only one countermeasure. It seams reasonable to assume that the overall benefit produced by a single countermeasure is the sum of the benefits that it produces when used to stop each attack action, but we to consider that this overall benefit can't be greater than the economic value of the asset it has to protect. For this reason we introduce the following definition:

Definition 6.6 The benefits produced by the use of a single countermeasure c to mitigate the loss produced by a set of attacks A, called ben_{Ac}, can be computed by using the following formula:

$$ben_{Ac} = \min\{AV, \sum_{a \in A} \big[ALE_a - \big(ALE_a \times (1 - RM_{ac})\big)\big]\}$$

where AV is the asset value, ALE_a is the annual loss produced by a and RM_{ac} is the risk mitigated by c. □

We use this definition to model a new scenario where we consider a single countermeasure to stop a set of attacks. Also in this case we have to change the definition of ROI as follows:

Definition 6.7 The Return on Investment associated to a countermeasure c able to mitigate the risks associated to a set A composed by m attacks is given by the following formula:

$$ROI_{Ac} = \frac{ben_{Ac} - CSI_c}{CSI_c} \tag{7}$$

where ben_{Ac} is the benefit produced by a countermeasure c and CSI_c is the cost of c. □

The following example shows how to compute ROI in this scenario.

Example 6.8 In this example we compute the profitability of a single countermeasure in mitigating attack strategies s_2, s_4 and s_5.
For instance, consider the countermeasure c_4, the RM associated to this countermeasure is 0.98 when c_4 is used to stop the attack strategies s_2 and s_5, while it is 0 when c_4 is used to stop the attacks s_4 so the benefit produced by c_4 is:

$$7000 - \big(7000 \times (1 - 0.98)\big) + 4000 - \big(4000 \times (1 - 0\%)\big) + 6000 - \big(6000 \times (1 - 0.98)\big) = 12740$$

the corresponding ROI results to be the highest among c_1, c_2, c_3, c_4, c_5 and c_6:

$$ROI_{(s_2,s_4,s_5),(c_4)} = \frac{12.740 - 450}{450} = 27.31$$

Table 4 shows the values of ROI associated to the other countermeasures.

Countermeasures	**ROI**
c_1	2.22
c_2	2.40
c_3	11.25
c_4	27.31
c_5	3.80
c_6	2.11

Table 4. The ROI associated to each countermeasure when it is used to mitigate the risk produced by all the possible attacks.

Return on Attack

This is another scenario that an attacker has to consider for the evaluation of an attack strategy when, in a system, only one countermeasure is able to mitigate the risks of a *set* of attacks. Once again we have to modify the definition of ROA as follows.

Definition 6.9 The Return on Attack, associated to a set of attack strategies A when there is a countermeasure c able to impair the attacks, can be computed by using the following formula:

$$ROA_{Ac} = \frac{GI - (GI \times RM_{Ac}) - cost_A}{cost_A} \tag{8}$$

where GI is the expected gain of the attack a, RM_{Ac} is the risk mitigated by c when it is used against A and is computed as: $RM_{Ac} = \min_{a \in A}(RM_{ac})$, and $cost_A$ is the sum of the costs associated to all the attacks action in the set A: $cost_A = \sum_{a \in A}(cost_a)$. □

In this case, from the attacker's point of view, the risk mitigated by a countermeasure c, is given by the minimum RM associated to the use of that countermeasure against all the attacks in the set: $\min_{a \in A}(RM_{ac})$. For instance, consider the scenario of Figure 2 and in particular the countermeasure c_1 "IDS", the value of $RM_{(s_2),(c_1)} = 0.69$ while the $RM_{(s_4),(c_1)} = RM_{(s_5),(c_1)} = 0$, so we suppose that the overall risk mitigated by c_1 is $RM_{(s_2,s_4,s_5),(c_1)} = 0$.

6.3 *Case (c): multiple attacks, multiple countermeasures*

Return on Investment

The last scenario that we identify (see Figure 5(c)) is composed by a set of countermeasures used to protect an asset of the system from a set of attacks.

Definition 6.10 The benefits produced by the use of a set of countermeasures C to mitigate the loss produced by a set of attacks A, called ben_{AC}, can be computed by using the following formula:

$$ben_{AC} = \min\{AV, \sum_{a \in A} \left[ALE_a - ALE_a \times \left(1 - RM_{aC}\right)\right]\}$$

where AV is the asset value, ALE_a is the annual loss associated to a and RM_{aC} is the risk mitigated by a set of countermeasures C. □

Notice that Definition 6.10 differs from Definition 6.6 because in this case we have to consider the benefits produced by a set of countermeasures C when they are used to mitigate the possible risks produced by each attack action a.

Changing the definition of ROI we obtain an overall evaluation of the entire scenario.

Definition 6.11 The Return on Investment associated to a set C composed by n countermeasures able to mitigate the risks associated to a set A composed by m attacks is given by the following formula:

$$ROI_{AC} = \frac{ben_{AC} - CSI_C}{CSI_C} \tag{9}$$

where ben_{AC} is the benefit produced by the set C used to stop the set of attacks A and CSI_C is the total cost associated to the set of countermeasures C: $CSI_C = \sum_{c \in C} CSI_c$. □

Example 6.12 In this example we compute the ROI associated to the possible sets of countermeasures in mitigating the risks associated to attacks a_1 and a_2.

Table B4 shows the values of ROI for all the sets. The set composed by the countermeasure c_4 is again the set with the highest value of ROI; also in this case the value of RM associated to c_1 and c_4 changes when they are used to stop the attack strategies s_2, s_4 or the attack s_5. So we obtain that the benefit is:

$$7000 - \big[7000 \times (1 - 0.98)\big] + 4000 - \big[4000 \times (1 - 0)\big] + 6000 - \big[6000 \times (1 - 0.98)\big] = 12740$$

and the corresponding ROI is:

$$ROI_{(s_2,s_4,s_5),(c_4)} = \frac{12740 - 450}{450} = 27.31$$

Return on Attack

The last scenario that the attacker has to consider is composed by a set of attack strategies to a single asset and a set of countermeasures introduced into the system to protect the asset itself (as shown in Figure 5(c)). In this case the ROA can be defined as follows.

Definition 6.13 The Return on Attack, associated to a set of attack strategies a when there is a set of countermeasures C able to mitigate the attacks, can be computed by using the following formula:

$$ROA_{AC} = \frac{GI - (GI \times RM_{AC}) - cost_A}{cost_A} \tag{10}$$

where GI is the expected gain of the attack a, RM_{AC} is the risk mitigated by the set C when is used against the set A and is computed as: $RM_{AC} = \min_{a \in A}(RM_{aC})$ and $cost_A = \sum_{a \in A}(cost_a)$. □

Using this definition we can determine what is the best attack's strategy considering the effects produced by all the possible defense configurations of a system. The following example shows how to use this new definition of ROA.

Example 6.14 In this example we analyze all the possible set of countermeasures that can be implemented into a system to defend the root of our defense tree.

Table B5 shows the values of ROA corresponding to each combination of countermeasures. We can see that in many cases the attacker obtains, using the three attack strategies, the highest value of ROA, for example:

$$ROA_{(s_2,s_4,s_5),(c_1,c_2)} = \frac{30000 - \big(30000 \times 0\big) - 3500}{3500} = 3.00$$

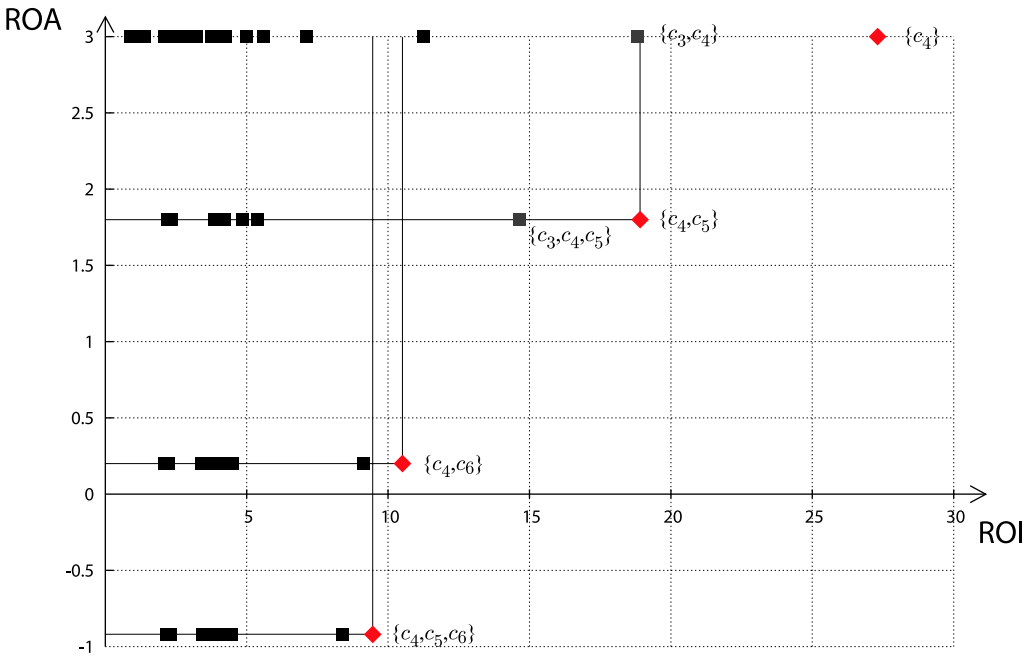

Figure 7. The *ROI* and *ROA* associated to each possible set of countermeasures when it is used to mitigate the risk produced by all the possible attacks.

7 Combining the defender's and the attacker's points of view

When the computation of *ROI* and *ROA* is complete, we can put together these indexes and perform a synthetic evaluation so as to determine the security investment that provides the best return on investment and that best discourages attacks.

The risk management process team should ideally select a countermeasure, or a set of countermeasures, that maximizes *ROI* and minimizes *ROA*. When such a countermeasure does not exist a countermeasure should be selected that: maximizes *ROI* (or minimizes *ROA*); or is any Pareto-optimal countermeasure; or maximizes a user-defined function of *ROI* and *ROA*.

A general procedure that could be used to select a set of countermeasures could be the following:

(a) to graphically represent all the sets and the corresponding values of *ROA* and *ROI* in order to provide the security manager with the complete view of the scenario;
(b) to discard sets having a negative value of *ROI*;
(c) to discard sets dominated by some other set of countermeasures, so as to consider only Pareto-optimal [28] sets;
(d) to choose the set with the highest value of *ROI* or the lowest value of *ROA*.

Consider, as an example, the graph of Figure 7 summarizing the results obtained by analyzing the last and more complex scenario that we show in this paper: the scenario with *multiple attacks*, *multiple countermeasures*. The x-axis displays the value of *ROI* associated to each set of countermeasures (see Table B4), while the y-axis displays the corresponding value of *ROA* (see Table B5).

The first thing that he can do is to eliminate, if any, sets with a negative value of *ROI* as they do not represent profitable investments. Then, he can discard dominated sets in such way that only the Pareto-optimal solutions are considered. For instance, considering our example, we can see that the set $\{c_4, c_5\}$ dominates several other sets like, for example, $\{c_3, c_4\}$ and $\{c_3, c_4, c_5\}$ (the first one has a higher value of *ROA*, while the second one has a lower value *ROI*). After this step some countermeasures can be discarded (those represented as black boxes in Figure 7). Finally, if the security manager wants to maximize *ROI*, the countermeasure (c_1) (use an IDS) will be selected, whilst if he/she prefers to minimize *ROA*, the selected set of countermeasures will be (c_4, c_5, c_6) (use an antivirus software, authenticate the IP address

and use an access control system).

8 Conclusions and future work

In this paper we presented our proposal for extending attack trees, a qualitative instrument used for modeling attack scenarios, with countermeasures and economic quantitative indexes. This extension allows us to evaluate effectiveness and profitability of countermeasures as well as their deterrent effect on attackers.

The methodology presented in this paper provides a basis for future work along several research directions. We plan to investigate how to leverage existing results on constraint semirings [3] and their use in attack trees rewriting [24] for computing attribute values of `and`/`or` nodes as functions of attribute values of their children in the considered defense tree. Results borrowed from probability [22] and possibility theory [11, 40] can also be useful for estimating frequency and likelihood of attacks from frequency and likelihood of vulnerabilities used in the attack.

The annual rate of occurrence (ARO) of attacks can be difficult to estimate, because organizations are typically reluctant to make attack data publicly available due to the negative influence this may have on their reputation. Thus, another interesting direction of research may consist in exploring how Return On Attack (ROA) and other information about the attacker, like, for example, non-economic motivation, risk attitude and type of attackers (which can range from script-kiddies to organized crime and cyberterrorist), can influence the annual rate of occurrence of attacks, also from a game theoretical perspective.

Other interesting extensions to the work presented in this paper include considering how vulnerabilities can be used for attacking multiple assets of an organization, how to replace fixed attribute values with constraints (e.g. intervals), and how to use fuzzy logic techniques to define functions combining ROI and ROA indexes. We hope our work can help encourage research and experimentation with use of economic indexes and combined development of attacker/defender perspectives during evaluation of alternative security investments.

References

[1] W. S. Baer and A. Parkinson. Cyberinsurance in it security management. *IEEE Security and Privacy*, 5(3):50–56, 2007.

[2] D. Balzarotti, M. Monga, and S. Sicari. Assessing the risk of using vulnerable components. In *1st Workshop on Quality of Protection*, Milan, Italy, September 2005.

[3] S. Bistarelli. *Semirings for Soft Constraint Solving and Programming*, volume 2969 of *LNCS*. Springer, 2004.

[4] S. Bistarelli, F. Fioravanti, and P. Peretti. Defense trees for economic evaluation of security investments. In *ARES*, pages 416–423, 2006.

[5] H. Bootsma, O. Curet, A. de Leeuw, A. Leijenhorst, W. Mocking, and D. Stewart. 2009 tmt global security survey. Technical report, Deloitte Touche Tohmatsu, 2009.

[6] S. Borg. Economically complex cyberattacks. *IEEE Security & Privacy*, 3(6):64–67, 2005.

[7] W. J. Caelli, D. Longley, and A. B. Tickle. A methodology for describing information and physical security architectures. In *IFIP/Sec '92: Proceedings of the IFIP TC11, Eigth International Conference on Information Security*, pages 277–296. North-Holland, 1992.

[8] J. Caulkins, E. D. Hough, N. R. Mead, and H. Osman. Optimizing investments in security countermeasures: A practical tool for fixed budgets. *IEEE Security and Privacy*, 5(5):57–60, 2007.

[9] H. Cavusoglu, B. Mishra, and S. Raghunathan. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *Int. J. Electron. Commerce*, 9(1):70–104, 2004.

[10] M. Cremonini and P. Martini. Evaluating information security investments from attackers perspective: the Return-On-Attack (ROA). In *Fourth Workshop on the Economics of Information Security*, June 2005.

[11] D. Dubois and H. Prade. *Possibility Theory: An Approach to the Computerized Processing of Uncertainty*. Plenum Press, 1988.
[12] F. Farahmand, S. B. Navathe, G. P. Sharp, and P. H. Enslow. A management perspective on risk of security threats to information systems. *Inf. Technol. and Management*, 6(2-3):203–225, 2005.
[13] N.L. Foster. *The application of software and safety engineering techniques to security protocol development*. PhD thesis, University of York, Department of Computer Science, 2002.
[14] M. Gilbert. Disaster recovery planning: Conducting a risk analysis. white paper 11, Hill Associates, 2003.
[15] L. Gordon and M. Loeb. Return on information security investments: Myths vs. realities. *Strategic Finance*, 84(5):26–31, 2002.
[16] L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, 5(4):438–457, 2002.
[17] Yacov Y. Haimes. *Risk Modeling, Assessment, and Management*. Wiley Publishing, 3rd edition, 2009.
[18] M. Howard and D. C. LeBlanc. *Writing Secure Code*. Microsoft Press, 2002.
[19] B. D. Jenkins. Security risk analysis and management. white paper, Norman Data Defense Systems, Inc., 1998.
[20] M. Krause and H. F. Tipton. *Handbook of Information Security Management*. Auerbach Publications, 1999.
[21] R. L. Krutz, R. D. Vines, and E. M. Stroz. *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*. Wiley, August 2001.
[22] D. V. Lindley. *Making Decisions*. John Wiley and Sons, 1985.
[23] P. Liu and W. Zang. Incentive-based modeling and inference of attacker intent, objectives, and strategies. In *CCS'03: Proceedings of the 10th ACM conference on Computer and Communications Security*, pages 179–189. ACM Press, 2003.
[24] S. Mauw and M. Oostdijk. Foundations of attack trees. In *8th Int. Conf. on Information Security and Cryptology*, LNCS. Springer, 2005.
[25] J. McDermott. Attack net penetration testing. In ACM Press, editor, *The 2000 New Security Paradigms Workshop ACM SIGSAC*, pages 15–22, 2000.
[26] J. W. Meritt. A method for quantitative risk analysis. In *Proceedings of the 22nd National Information Systems Security Conference*, October 1999.
[27] A. Moore, R. Ellison, and R. Linger. Attack modeling for information security and survivability. Technical report, Software Engineering Institute CMU/SEI-2001-TN-001, 2001.
[28] V. Pareto. *Manual of Political Economy*. Augustus M. Kelley, 1971. orig. (1960) in Italian.
[29] S. L. Pfleeger and R. Rue. Cybersecurity economic issues: Clearing the path to good practice. *IEEE Software*, 25(1):35–42, 2008.
[30] N. C. Rasmussen. Reactor safety study: An assessment of accident risks in us commercial nuclear power plants. Technical report, Nuclear Regulatory commission, 1975.
[31] R. Richardson. Csi computer crime and security survey. Technical report, CSI, Computer Security Institute, 2007.
[32] S. Schechter. Quantitatively differentiating system security. In *1st Workshop Economics of Information Security*, 2002.
[33] S. E. Schechter. *Computer Security Strength & Risk: A Quantitative Approach*. PhD thesis, Harvard University, May 2004.
[34] B. Schneier. Attack trees: Modeling security threats. Dr. Dobb's Journal, 1999.
[35] B. Schneier. *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000.
[36] W. Sonnenreich, J. Albanese, and B. Stout. Return On Security Investment (ROSI): A practical quantitative model. In *Security in Information Systems, Proceedings of the 3rd International Workshop on Security in Information Systems, WOSIS 2005, In conjunction with ICEIS2005*, pages 239–252. INSTICC Press, 2005.
[37] K. J. Soo Hoo. How much is enough: a risk management approach to computer security. In *Workshop on Economics and Information Security*, 2002.
[38] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology

systems. Nist special publication 800–30, NIST, National Institute of Standard Technology, July 2002.

[39] H. A. Watson. Launch control safety study. Technical report, Bell Telephone Laboratories, 1961.

[40] L. A. Zadeh. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems*, I:3–28, 1978.

Appendix A: A detailed of the use of the algorithm `AttackStrategies` considering the attack tree depicted in Figure 1.

As an example of the use of the algorithm `AttackStrategies` consider the attack tree depicted in Figure 1. The algorithm starts initializing the set $AS = \emptyset$, a first strategy $s_1 = \{root\}$ and adding s_1 to the set Sol, then each attack action contained in each set s_i is checked.

First iteration: the set s_1 is considered. s_1 contains only the *root*, the *root* is not a leaf of the tree so the algorithm checks its type; it is an `or`-node so the solution s_1 is duplicated in Sol twice (because *root* has two children). In the first new solution, s_2, the node *root* is replaced by its first child (a_1) while in the second new solution, s_3 it is replaced by its second child (a_2). At the end of this iteration we have that $Sol = \{s_2, s_3\}$, $s_2 = \{a_1\}$ and $s_3 = \{a_2\}$.

Second iteration: the set s_2 is considered. s_2 contains only the node a_1. a_1 is not a leaf so its type is checked, it is a `and`-node so it is replaced in s_2 by all its children: a_3, a_4, a_5 and a_6. In this way we have that $Sol = \{s_2, s_3\}$, $s_2 = \{a_3, a_4, a_5, a_6\}$ and $s_3 = \{a_2\}$.

Third iteration: the set s_3 is considered. s_3 contains only the node a_2. It is not a leaf of the tree so the algorithm checks its type; a_2 is an `or`-node so s_3 is duplicated in Sol twice (because a_2 has two children). In the first new solution, s_4, the node a_2 is replaced by the node a_7 while in the second new solution, s_5, the node a_2 is replaced by a_8. The set s_3 is removed from Sol. At the end of this iteration we have that $Sol = \{s_2, s_4, s_5\}$, $s_2 = \{a_3, a_4, a_5, a_6\}$, $s_4 = \{a_7\}$ and $s_5 = \{a_8\}$.

Fourth iteration: the set s_2 is considered. $s_2 = \{a_3, a_4, a_5, a_6\}$ contains only leaves of the tree, so the algorithm adds s_2 to the set of attack strategies AS and removes it to the set Sol. At the end of this iteration we have that $AS = \{s_2\}$, $Sol = \{s_4, s_5\}$, $s_2 = \{a_3, a_4, a_5, a_6\}$, $s_4 = \{a_7\}$ and $s_5 = \{a_8\}$.

Fifth iteration: the set s_4 is considered. $s_4 = \{a_7\}$ contains only a leaf so so the algorithm adds s_4 to the set of attack strategies AS and removes it to the set Sol. At the end of this iteration we have that $AS = \{s_2, s_4\}$, $Sol = \{s_5\}$, $s_2 = \{a_3, a_4, a_5, a_6\}$, $s_4 = \{a_7\}$ and $s_5 = \{a_8\}$.

Sixth iteration: the set s_5 is considered. $s_5 = \{a_8\}$ contains only a leaf so so the algorithm adds s_5 to the set of attack strategies AS and remove it to the set Sol. At the end of this iteration we have that $AS = \{s_2, s_4, s_5\}$, $Sol = \emptyset$, $s_2 = \{a_3, a_4, a_5, a_6\}$, $s_4 = \{a_7\}$ and $s_5 = \{a_8\}$.

Summarizing, the algorithm returns the set AS containing the three attack strategies represented in attack tree of Figure 1: $s_2 = \{a_3, a_4, a_5, a_6\}$ representing a Denial of Service attack, $s_4 = \{a_7\}$ representing a theft of proprietary information by a man in the middle attack and $s_5 = \{a_8\}$ representing a theft of proprietary information by phishing.

Appendix B: List of tables

B.1 *Case (a): single attack, multiple countermeasures*

The following tables show the *ROI* associated to different sets of countermeasures when they are used to mitigate the risk produced by a single attack action. In particular they represent the *denial of services* attack (Table B1), the *man in the middle* attack (Table B2) and finally the *phishing* attack (Table B3).

B.2 *Case (c): multiples attack strategy, multiple countermeasures*

The following tables show the *ROI* and the *ROA* associated to different sets of countermeasures when they are used to mitigate the risk produced by a set of attack actions. In particular Table B4 shows the ROI and Table B5 shows the ROA.

Countermeasures	ROI	Countermeasures	ROI	Countermeasures	ROI
c_1	2.22	c_1, c_2, c_3	0.89	c_1, c_2, c_3, c_5	0.77
c_2	2.40	c_1, c_2, c_4	0.77	c_1, c_2, c_3, c_6	0.52
c_3	11.25	c_1, c_2, c_5	0.87	c_1, c_2, c_4, c_5	0.67
c_4	14.24	c_1, c_2, c_6	0.59	c_1, c_2, c_4, c_6	0.44
c_5	-1.00	c_1, c_3, c_4	2.26	c_1, c_2, c_5, c_6	0.51
c_6	-1.00	c_1, c_3, c_5	2.59	c_1, c_3, c_5, c_6	1.46
c_1, c_2	1.00	c_1, c_3, c_6	1.69	c_1, c_3, c_4, c_5	1.92
c_1, c_3	3.12	c_1, c_4, c_5	2.18	c_1, c_3, c_4, c_6	1.30
c_1, c_4	2.59	c_1, c_4, c_6	1.46	c_1, c_4, c_5, c_6	1.26
c_1, c_5	1.76	c_1, c_5, c_6	0.82	c_2, c_3, c_4, c_5	1.41
c_1, c_6	1.01	c_2, c_3, c_4	1.01	c_2, c_3, c_4, c_6	0.97
c_2, c_3	2.18	c_2, c_3, c_5	1.86	c_2, c_3, c_5, c_6	1.09
c_2, c_4	1.86	c_2, c_3, c_6	1.26	c_2, c_4, c_5, c_6	0.94
c_2, c_5	2.02	c_2, c_4, c_5	1.59	c_3, c_4, c_5, c_6	2.89
c_2, c_6	1.34	c_2, c_4, c_6	1.09	c_1, c_2, c_3, c_4, c_5	0.59
c_3, c_4	9.77	c_2, c_5, c_6	1.16	c_1, c_2, c_3, c_4, c_6	0.39
c_3, c_5	4.44	c_3, c_4, c_5	6.78	c_1, c_2, c_3, c_5, c_6	0.44
c_3, c_6	1.23	c_3, c_4, c_6	3.52	c_1, c_2, c_4, c_5, c_6	0.37
c_4, c_5	8.80	c_3, c_5, c_6	0.81	c_1, c_3, c_4, c_5, c_6	1.12
c_4, c_6	4.08	c_4, c_5, c_6	3.29	c_2, c_3, c_4, c_5, c_6	0.84
c_5, c_6	-1.00	c_1, c_2, c_3, c_4	0.69	c_1, c_2, c_3, c_4, c_5, c_6	0.32

Table B1. *Denial of services* attack.

Countermeasures	ROI	Countermeasures	ROI	Countermeasures	ROI
c_1	-1.00	c_1, c_2, c_3	-1.00	c_1, c_2, c_3, c_5	-0.70
c_2	-1.00	c_1, c_2, c_4	-1.00	c_1, c_2, c_3, c_6	-0.39
c_3	-1.00	c_1, c_2, c_5	-0.68	c_1, c_2, c_4, c_5	-0.71
c_4	-1.00	c_1, c_2, c_6	-0.36	c_1, c_2, c_4, c_6	-0.42
c_5	3.80	c_1, c_3, c_4	-1.00	c_1, c_2, c_5, c_6	-0.14
c_6	2.11	c_1, c_3, c_5	-0.38	c_1, c_3, c_5, c_6	0.40
c_1, c_2	-1.00	c_1, c_3, c_6	0.08	c_1, c_3, c_4, c_5	-0.50
c_1, c_3	-1.00	c_1, c_4, c_5	-0.45	c_1, c_3, c_4, c_6	-0.08
c_1, c_4	-1.00	c_1, c_4, c_6	-0.02	c_1, c_4, c_5, c_6	0.29
c_1, c_5	-0.31	c_1, c_5, c_6	0.51	c_2, c_3, c_4, c_5	-0.59
c_1, c_6	0.17	c_2, c_3, c_4	0.17	c_2, c_3, c_4, c_6	-0.21
c_2, c_3	-1.00	c_2, c_3, c_5	-0.51	c_2, c_3, c_5, c_6	0.19
c_2, c_4	-1.00	c_2, c_3, c_6	-0.10	c_2, c_4, c_5, c_6	0.11
c_2, c_5	-0.47	c_2, c_4, c_5	-0.56	c_3, c_4, c_5, c_6	1.22
c_2, c_6	-0.03	c_2, c_4, c_6	-0.16	c_1, c_2, c_3, c_4, c_5	-0.73
c_3, c_4	-1.00	c_2, c_5, c_6	0.27	c_1, c_2, c_3, c_4, c_6	-0.45
c_3, c_5	1.67	c_3, c_4, c_5	0.33	c_1, c_2, c_3, c_5, c_6	-0.18
c_3, c_6	1.55	c_3, c_4, c_6	0.81	c_1, c_2, c_4, c_5, c_6	-0.22
c_4, c_5	0.71	c_3, c_5, c_6	1.96	c_1, c_3, c_4, c_5, c_6	0.21
c_4, c_6	1.07	c_4, c_5, c_6	1.50	c_2, c_3, c_4, c_5, c_6	0.05
c_5, c_6	2.48	c_1, c_2, c_3, c_4	-1.00	c_1, c_2, c_3, c_4, c_5, c_6	-0.25

Table B2. *Man in the middle* attack.

Countermeasures	ROI	Countermeasures	ROI	Countermeasures	ROI
c_1	3.00	c_1, c_2, c_3	3.00	c_1, c_2, c_3, c_5	3.00
c_2	3.00	c_1, c_2, c_4	3.00	c_1, c_2, c_3, c_6	3.00
c_3	3.00	c_1, c_2, c_5	3.00	c_1, c_2, c_4, c_5	1.80
c_4	3.00	c_1, c_2, c_6	3.00	c_1, c_2, c_4, c_6	0.20
c_5	3.00	c_1, c_3, c_4	3.00	c_1, c_2, c_5, c_6	3.00
c_6	3.00	c_1, c_3, c_5	3.00	c_1, c_3, c_5, c_6	3.00
c_1, c_2	3.00	c_1, c_3, c_6	3.00	c_1, c_3, c_4, c_5	1.80
c_1, c_3	3.00	c_1, c_4, c_5	1.80	c_1, c_3, c_4, c_6	0.20
c_1, c_4	3.00	c_1, c_4, c_6	0.20	c_1, c_4, c_5, c_6	-0.92
c_1, c_5	3.00	c_1, c_5, c_6	3.00	c_2, c_3, c_4, c_5	1.80
c_1, c_6	3.00	c_2, c_3, c_4	3.00	c_2, c_3, c_4, c_6	0.20
c_2, c_3	3.00	c_2, c_3, c_5	3.00	c_2, c_3, c_5, c_6	3.00
c_2, c_4	3.00	c_2, c_3, c_6	3.00	c_2, c_4, c_5, c_6	-0.92
c_2, c_5	3.00	c_2, c_4, c_5	1.80	c_3, c_4, c_5, c_6	-0.92
c_2, c_6	3.00	c_2, c_4, c_6	0.20	c_1, c_2, c_3, c_4, c_5	1.80
c_3, c_4	3.00	c_2, c_5, c_6	3.00	c_1, c_2, c_3, c_4, c_6	0.20
c_3, c_5	3.00	c_3, c_4, c_5	1.80	c_1, c_2, c_3, c_5, c_6	3.00
c_3, c_6	3.00	c_3, c_4, c_6	0.20	c_1, c_2, c_4, c_5, c_6	-0.92
c_4, c_5	1.80	c_3, c_5, c_6	3.00	c_1, c_3, c_4, c_5, c_6	-0.92
c_4, c_6	0.20	c_4, c_5, c_6	-0.92	c_2, c_3, c_4, c_5, c_6	-0.92
c_5, c_6	3.00	c_1, c_2, c_3, c_4	3.00	c_1, c_2, c_3, c_4, c_5, c_6	-0.92

Table B3. *Phishing* attack.

Countermeasures	ROI	Countermeasures	ROI	Countermeasures	ROI
c_1	2.22	c_1, c_2, c_3	0.89	c_1, c_2, c_3, c_5	1.08
c_2	2.40	c_1, c_2, c_4	2.26	c_1, c_2, c_3, c_6	1.13
c_3	11.25	c_1, c_2, c_5	1.19	c_1, c_2, c_4, c_5	2.35
c_4	27.31	c_1, c_2, c_6	1.23	c_1, c_2, c_4, c_6	2.23
c_5	3.80	c_1, c_3, c_4	4.99	c_1, c_2, c_5, c_6	1.37
c_6	2.11	c_1, c_3, c_5	3.21	c_1, c_3, c_5, c_6	2.86
c_1, c_2	1.00	c_1, c_3, c_6	2.77	c_1, c_3, c_4, c_5	4.87
c_1, c_3	3.12	c_1, c_4, c_5	5.40	c_1, c_3, c_4, c_6	4.14
c_1, c_4	5.61	c_1, c_4, c_6	4.50	c_1, c_4, c_5, c_6	4.45
c_1, c_5	2.45	c_1, c_5, c_6	2.33	c_2, c_3, c_4, c_5	3.86
c_1, c_6	2.18	c_2, c_3, c_4	2.18	c_2, c_3, c_4, c_6	3.42
c_2, c_3	2.18	c_2, c_3, c_5	2.35	c_2, c_3, c_5, c_6	2.28
c_2, c_4	4.26	c_2, c_3, c_6	2.16	c_2, c_4, c_5, c_6	3.69
c_2, c_5	2.55	c_2, c_4, c_5	4.21	c_3, c_4, c_5, c_6	8.38
c_2, c_6	2.31	c_2, c_4, c_6	3.68	c_1, c_2, c_3, c_4, c_5	2.20
c_3, c_4	18.82	c_2, c_5, c_6	2.43	c_1, c_2, c_3, c_4, c_6	2.10
c_3, c_5	7.11	c_3, c_4, c_5	14.64	c_1, c_2, c_3, c_5, c_6	1.27
c_3, c_6	3.77	c_3, c_4, c_6	9.12	c_1, c_2, c_4, c_5, c_6	2.31
c_4, c_5	18.91	c_3, c_5, c_6	3.78	c_1, c_3, c_4, c_5, c_6	4.12
c_4, c_6	10.51	c_4, c_5, c_6	9.46	c_2, c_3, c_4, c_5, c_6	3.44
c_5, c_6	2.48	c_1, c_2, c_3, c_4	2.10	c_1, c_2, c_3, c_4, c_5, c_6	2.18

Table B4. *ROI*.

Countermeasures	ROA	Countermeasures	ROA	Countermeasures	ROA
c_1	3.00	c_1, c_2, c_3	3.00	c_1, c_2, c_3, c_5	3.00
c_2	3.00	c_1, c_2, c_4	3.00	c_1, c_2, c_3, c_6	3.00
c_3	3.00	c_1, c_2, c_5	3.00	c_1, c_2, c_4, c_5	1.80
c_4	3.00	c_1, c_2, c_6	3.00	c_1, c_2, c_4, c_6	0.20
c_5	3.00	c_1, c_3, c_4	3.00	c_1, c_2, c_5, c_6	3.00
c_6	3.00	c_1, c_3, c_5	3.00	c_1, c_3, c_5, c_6	3.00
c_1, c_2	3.00	c_1, c_3, c_6	3.00	c_1, c_3, c_4, c_5	1.80
c_1, c_3	3.00	c_1, c_4, c_5	1.80	c_1, c_3, c_4, c_6	0.20
c_1, c_4	3.00	c_1, c_4, c_6	0.20	c_1, c_4, c_5, c_6	-0.92
c_1, c_5	3.00	c_1, c_5, c_6	3.00	c_2, c_3, c_4, c_5	1.80
c_1, c_6	3.00	c_2, c_3, c_4	3.00	c_2, c_3, c_4, c_6	0.20
c_2, c_3	3.00	c_2, c_3, c_5	3.00	c_2, c_3, c_5, c_6	3.00
c_2, c_4	3.00	c_2, c_3, c_6	3.00	c_2, c_4, c_5, c_6	-0.92
c_2, c_5	3.00	c_2, c_4, c_5	1.80	c_3, c_4, c_5, c_6	-0.92
c_2, c_6	3.00	c_2, c_4, c_6	0.20	c_1, c_2, c_3, c_4, c_5	1.80
c_3, c_4	3.00	c_2, c_5, c_6	3.00	c_1, c_2, c_3, c_4, c_6	0.20
c_3, c_5	3.00	c_3, c_4, c_5	1.80	c_1, c_2, c_3, c_5, c_6	3.00
c_3, c_6	3.00	c_3, c_4, c_6	0.20	c_1, c_2, c_4, c_5, c_6	-0.92
c_4, c_5	1.80	c_3, c_5, c_6	3.00	c_1, c_3, c_4, c_5, c_6	-0.92
c_4, c_6	0.20	c_4, c_5, c_6	-0.92	c_2, c_3, c_4, c_5, c_6	-0.92
c_5, c_6	3.00	c_1, c_2, c_3, c_4	3.00	c_1, c_2, c_3, c_4, c_5, c_6	-0.92

Table B5. *ROA*.