Strategic games on defense trees*

Stefano Bistarelli[1,2], Marco Dall'Aglio[1], and Pamela Peretti[1]

[1] Dipartimento di Scienze, Università degli Studi "G. d'Annunzio", Pescara, Italy
{bista,maglio,peretti}@sci.unich.it

[2] Istituto di Informatica e Telematica, CNR, Pisa, Italy
Stefano.Bistarelli@iit.cnr.it

Abstract. In this paper we use defense trees, an extension of attack trees with countermeasures, to represent attack scenarios and game theory to detect the most promising actions attacker and defender. On one side the attacker wants to break the system (with as little efforts as possible), on the opposite side the defender want to protect it (sustaining the minimum cost).
As utility function for the attacker and for the defender we consider economic indexes (like the Return on Investment (ROI) and the Return on Attack (ROA)). We show how our approach can be used to evaluate effectiveness and economic profitability of countermeasures as well as 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.

Key words: Security, Risk Analysis, Game Theory

1 Introduction

Security has become today a fundamental part of the enterprise investment. 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 on the real and concrete threats 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 the process is to make security managers aware of the possible risks, and to guide them toward the adoption of a set of countermeasures which 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 task. There are no standard methodologies for the process, and often security managers have to decide among too many alternatives.

To model the attack scenario and the defender possibilities we use *defense trees* [1], an extension of attacks trees with countermeasures. The vulnerabilities are represented as leaf nodes of the tree and are decorated with the countermeasures able to mitigate the damage of threats using such a vulnerability.

* Partially supported by the MIUR PRIN 2005-015491.

Moreover, economic indexes are used as labels for countermeasures and attacks. The *Return on Investment* (ROI) [18, 17] 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) [3] is instead an index that is aimed at measuring the convenience of attacks, by considering the impact of a security solution on the attacker's behavior.

The computed ROI and ROA function are then considered as utility functions (payoffs) in a two player strategic game. On one side the system administrator wants to protect the system by buying and adopting countermeasures; on the other side the attacker wants to exploit the vulnerabilities and obtain some profit by breaking the system.

We solve the games by looking at their Nash equilibria with both pure and mixed strategies. Our results show that is always worth installing countermeasures for the defender; however, it is not true that increasing the number of countermeasure gives an overall better benefit to the enterprise (as showed in [7] investing in security measure is not profitable beyond a certain level). This is not completely surprising, since more and more sophisticated protection may be accompanied by escalating marginal costs, while the probability that any given type of protection will be needed (that is, its expected benefit) may remain constant. Also interesting is the fact that the strategies of *no-attacks* and *no-countermeasures* is not (unfortunately) a point of equilibrium.

After an introduction to the concepts of security risk management and of defense trees (Section 2) we study the selection of the most promising countermeasures by interpreting the scenario as a game with two players: the defender and the attacker (Section 3). Section 4, instead, shows a realistic example where the attacker wants to steal information about customers maintained in a server. Finally, Section 5 summarizes the paper results and sketches some directions for future work.

2 Security risk management and defense trees

Defending an IT system is hard because many are the risks that can affect each asset of the system. Organizations need a process that enable to identify, describe and analyze the possible vulnerability that can be exploited by an adverse individual, and identify the security measures necessary to reduce the risks.

In [1] we propose the use of the *defense tree* (extension of *attack trees* [15, 16]), an instrument for representing an attack against a system and how it can be mitigated by a set of countermeasures.
The difference between an attack tree and a defense tree is that the first represents only the attack strategies that an attacker can perform, while the second adds the set of countermeasures that can be introduced into the system to mitigate the possible damages produced by an attack.

Integrating countermeasures into threat trees, and more generally into directed acyclic graphs, is not new. In the early 90s researchers used "threat countermeasure diagrams". One may also see examples of countermeasures in DAGs

in both Nathalie Foster's thesis [4] and Stuart Schechter's thesis [14], both of which include discussions and histories of the evolution of these structures. Even in the popular Microsoft text by Howard and LeBlanc, "Writing Secure Code", one can find threat trees (another name for attack trees) in which countermeasures are integrated [8].

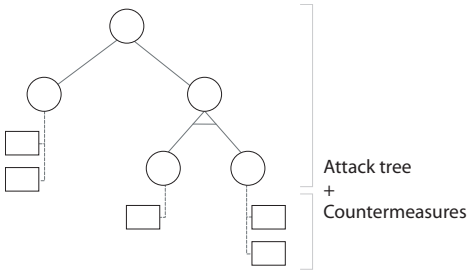


Fig. 1. A *defense tree.*

Figure 1 shows an example of a defense tree: round nodes form the attack tree and square nodes represent the corresponding countermeasures. The root of the tree is associated with an asset of the IT system under consideration and represents the attacker's goal. Leaf nodes in the attack tree represent simple subgoals which lead the attacker to (partially) damage the asset by exploiting a single vulnerability. Non-leaf nodes (including the tree root) can be of two different types: `or`-nodes and `and`-nodes. Subgoals associated with `or`-nodes are completed as soon as any of its child nodes is achieved, while `and`-nodes represent subgoals which require all of its child nodes to be completed (in Figure 1 we draw an horizontal line between the children of an `and`-node to distinguish it from the `or`-node).

We consider defense trees [1] enriched with economic indexes that quantify the cost of attacks and the return on security investments in any branch of the tree. We interpret such indexes as utility functions for the system administrator and for the attacker, by viewing the scenario as a classical game with two player looking for different and usually opposite results (see Section 3).

In particular we label the tree with:

1. the *Return On Investment* (ROI) [17] measuring the return that a defender expects from a security investment over the costs he sustains for countermeasures. It is calculated with the formula:

$$ROI = \frac{ALE \times RM - CSI}{CSI}$$

   where:
   - the *Annualized Loss Expectancy* (ALE) [9] measures the expected annual financial loss which can be ascribed to a threat to the organization. It is calculated as $ALE = AV \times EF \times ARO$, where:

    - the *Asset Value* (AV) is a measure of the cost of creation, development, support, replacement and ownership values of an asset,
    - the *Exposure Factor* (EF) represents a measure of the magnitude of loss or impact on the value of an asset arising from a threat (expressed as a percentage of the asset value),
    - the *Annualized Rate of Occurrence* (ARO) is a number that represents the estimated number of annual occurrences of a threat.
  - the *Risk Mitigated* by a countermeasure (RM) represents the effectiveness of a countermeasure in mitigating the risk of loss deriving from exploiting a vulnerability (RM is a numeric value in [0,1] that measures the proportion of reduced risk),
  - the *Cost of Security Investment* (CSI) is the cost that an enterprise sustains for implementing a given countermeasure.
2. the *Return On Attack* (ROA) [3] measures the gain that an attacker expects from a successful attack over the losses that he sustains due to the adoption of security measures by his target. It is calculated as:

$$ROA = \frac{GI \times (1 - RM) - (cost_a + cost_{ac})}{cost_a + cost_{ac}}$$

   where:
   - GI is the expected gain from the successful attack on the specified target,
   - $cost_a$ is the cost sustained by the attacker to succeed,
   - $cost_{ac}$ is the additional cost brought by the countermeasure c adopted by the defender to mitigate the attack a.

We will see in Section 3 that other choices for the utility functions are possible. For instance we could consider ROI and ROA without dividing the gain by the costs (CSI and $cost_a + cost_{ac}$ respectively), or by considering the damage of an attack without considering its (often unknown) rate of occurrence (ARO).

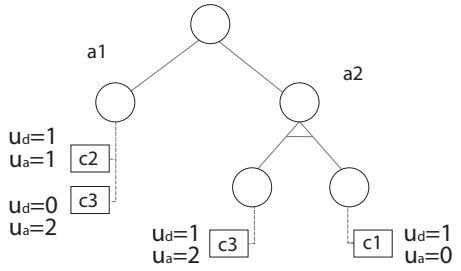
3 Defense trees as strategic games

In this section we will show how game theory can be used to analyze the possible strategies of the system administrator and of the attacker. In our scenario we consider a strategic game [6] that consists of:

- n players (n is usually just 2, but we plan to extend it to the case of 1 defender and k attackers),
- a set of strategies S_i for each player i,
- the utility function (or payoff) u_i for each player i.

We consider here the case with $n = 2$ players: the *defender* (Bob) and the *attacker* (Alice) of a system. The set of defender's strategies is the set of countermeasures that he can introduce into the systems while the set of attacker's strategies is the set of vulnerability that she can exploit. The payoff functions we will consider are the Return on Investment (ROI) for the defender and the

Return on Attack (ROA) for the attacker. Notice that ROI and ROA represent normalized payoffs; in some cases a not normalized utility function could be used instead, that may lead to different equilibrium strategies (because each player is trying to maximize its return rather than its payoff).



(a) Defence tree.

	a1	a2
c1	1,1	1,0
c2	1,1	0,2
c3	0,2	1,2

(b) Strategic game.

Fig. 2. Defense tree and the corresponding strategic game (with a pure strategy Nash Equilibrium).

As an example consider the defense tree depicted in Figure 2(a). It can be modeled as the strategic game in Figure 2(b), where:

- the players of the game are the defender of the enterprise that can select actions represented in the rows, and the attacker that can choose possible attacks (represented as columns in the table),
- the defender's set of strategies is $S_d = \{c_1, c_2, c_3\}$, that consists of the possible countermeasures that he can enforce to protect the system,
- the attacker's set of action is $S_a = \{a_1, a_2\}$ that represents the two possible attack strategies (the columns in Figure 2(b));
- the goal of each player is to maximize his/her own payoff function (the number in each box of Figure 2(b)). The payoffs associated to a strategy (c_i, a_i) are $u_d(c_i, a_i)$ for the defender, and $u_a(c_i, a_i)$ for the attacker.

Each player chooses the best available action given his belief about the other player's action.

The solution of the game is the (set of) countermeasure that the defender is more likely to adopt, and the (set of) vulnerability that the attacker feels more suitable to exploit. In some special cases the best strategy of the attacker and of the defender converges to a specific action profile s^* with the property that the defender cannot do better by choosing an action different from s_d^*, given that the attacker adopt s_a^*, and viceversa. In this case we say that the game admits a *Nash Equilibrium* [13].

Definition 1 (Nash Equilibrium [6]). *In a strategic game with* 2 *players, consider the sets* S_1, S_2 *and the functions* u_1, u_2 *that are the set of possible*

strategies and the utility functions of players 1 *and* 2 *respectively. The combination of strategy* (s_1^*, s_2^*) *with* $s_1^* \in S_1$ *and* $s_2^* \in S_2$ *is a Nash Equilibrium if and only if, for each player* i*, the action* s_i^* *is the best response to the other player:*

$$u_1(s_1^*, s_2^*) \geq u_1(s_1, s_2^*) \text{ for any } s_1 \in S_1$$

$$u_2(s_1^*, s_2^*) \geq u_2(s_1^*, s_2) \text{ for any } s_2 \in S_2$$

Figure 2(a) shows an example of defense tree where two possible attacks are represented: a_1 and a_2. The first one can be mitigated by two countermeasure c_2 and c_3, the second one can be mitigated by c_1 and c_3. Figure 2(b) shows the corresponding strategic game, where the numbers in the bimatrix are the payoffs associated to each player (associated as label to the tree as we will see in Section 3).

Using Definition 1 we can calculate the possible Nash Equilibria of the game. Notice that if the attacker plays strategy a_1 the best response for the defender is to play the strategies c_1 or c_2 (by looking at the first column on the left we can see that he can gain 1 instead of 0), while if the attacker plays strategy a_2 the best response is to play the strategies c_1 or c_3.
Conversely if the defender plays the strategy c_1 the best response for the attacker is play strategy a_1, if the defender plays the strategy c_2 the best response is to play strategy a_2 and if the defender plays strategy c_3 the best response for the attacker is to play strategies a_1 or a_2. The game admits two different Nash Equilibria (the circled payoffs): the couple of strategies $\{c_1, a_1\}$ and $\{c_3, a_2\}$.

The Nash Equilibrium represents the best strategies for both the attacker and the defender (with the hypothesis that neither the attacker nor the defender have any knowledge of the other). In the case depicted in Figure 2, the defender will select, if possible, both countermeasure $c1$ and $c3$. However if the financial resources available to the system administrator are limited, only countermeasure $c3$ will be selected (because it will cover both strategy of the attacks). In Section 4 a complete more realistic example will be presented where the economic indexes will be used for the selection.

Sometimes in a strategic game it is impossible to find a Nash Equilibrium. Moreover we often need to take into account the uncertainty of the player's behavior. In this case a player may consider a *mixed strategy.*

Definition 2 (Mixed strategy [6]). *Consider a strategic game with* 2 *players,* $G = \{S_1, S_2; u_1, u_2\}$ *where* $S_i = \{s_{i1}, \ldots, s_{ik}\}$ *the strategies of player* i*. A* mixed strategy *for player* $1 \leq i \leq 2$ *is a probability distribution* $p_i = (p_{i1}, \ldots, p_{ik})$*, where* $0 \leq p_{ik}$*.*

In our context the use of mixed strategies finds a justification in the fact that a player, especially the defender, deals with a single attacker, whose behavior is not known. He may assume, however, that this players is drawn from a population of attackers whose actions can be estimated as frequencies from previous attacks (leading to the notion of *repeated games* where the players can randomize their strategies).

What we obtain is shown in Figure 3. The Attacker A can play the strategy a_1 with probability p_{a_1}, and the strategy a_2 with probability p_{a_2}, whilst the Defender D plays the strategy c_i with probability p_{c_i}, with $1 \leq i \leq 3$.

		p_{a_1}	p_{a_2}
		a_1	a_2
p_{c_1}	c_1	$u_d(c_1,a_1), u_a(c_1,a_1)$	$u_d(c_1,a_2), u_a(c_1,a_2)$
p_{c_2}	c_2	$u_d(c_2,a_1), u_a(c_2,a_1)$	$u_d(c_2,a_2), u_a(c_2,a_2)$
p_{c_3}	c_3	$u_d(c_3,a_1), u_a(c_3,a_1)$	$u_d(c_3,a_2), u_a(c_3,a_2)$

Fig. 3. Mixed strategies.

We can compute payoffs in presence of mixed strategies by taking into account probability distributions and computing expectations. If the defender uses a pure strategy [3] in response to a mixed strategy of the attacker, the resulting payoffs for each possible countermeasure c_i is:

$$u_d(c_i) = u_d(c_i, a_1) \times p_{a_1} + u_d(c_i, a_2) \times p_{a_2}$$

If the attacker uses a pure strategy in response of a mixed strategy of the defender the resulting payoffs for each attack a_i is:

$$u_a(a_i) = u_a(c_1, a_i) \times p_{c_1} + u_a(c_2, a_i) \times p_{c_2} + u_a(c_3, a_i) \times p_{c_3}$$

Definition 3. *Given a game with 2 players, and 2 sets of strategies* $S_1 = \{s_{11}, \ldots, s_{1K_1}\}$ *and* $S_2 = \{s_{21}, \ldots, s_{2K_2}\}$*, if player* i *believes that player* j *will play the strategies* $(s_{j1}, \ldots, s_{jK_j})$ *with probability* $(p_{j1}, \ldots, p_{jK_j})$*, the expected payoff for player* i *obtained with the pure strategy* s_{ij} *is:*

$$\sum_{k=1}^{K_j} p_{jk} u_i(s_{ij}, s_{jk})$$

We can use Definition 3 to solve the game in Figure 2 by using the mixed strategies. In particular suppose that the defender uses a pure strategy and the attacker plays a mixed strategy $\{a_1, a_2\}$ with probability (p_{a_1}, p_{a_2}) (as shown in Figure 4). The expected payoff for the defender, if the attacker plays a mixed strategy are:

$$\begin{aligned} &1 \cdot p_{a_1} + 1 \cdot p_{a_2} = p_{a_1} + p_{a_2} && \text{for countermeasure } c_1 \\ &1 \cdot p_{a_1} + 0 \cdot p_{a_2} = p_{a_1} && \text{for countermeasure } c_2 \\ &0 \cdot p_{a_1} + 1 \cdot p_{a_2} = p_{a_2} && \text{for countermeasure } c_3 \end{aligned}$$

[3] A pure strategy is a strategy that a player plays with probability 1.

	p_{a1} a_1	p_{a2} a_2
p_{c1} c_1	1,1	1,0
p_{c2} c_2	1,1	0,2
p_{c3} c_3	0,2	1,2

Fig. 4. Example of mixed strategy.

Conversely, if the attacker uses a pure strategy and the defender plays a mixed strategy $\{c_1, c_2, c_3\}$ with probability $(p_{c_1}, p_{c_2}, p_{c_3})$, the expected payoff for the defender are:

$$\begin{aligned} 1 \cdot p_{c_1} + 1 \cdot p_{c_2} + 2 \cdot p_{c_3} &= p_{c_1} + p_{c_2} + 2p_{c_3} \text{ for attack } a_1 \\ 0 \cdot p_{c_1} + 2 \cdot p_{c_2} + 2 \cdot p_{c_3} &= 2p_{c_2} + 2p_{c_3} \quad \text{for attack } a_2 \end{aligned}$$

Definition 4. *If the players* 1 *and* 2 *play respectively the strategies* $(s_{11}, \ldots, s_{1J})$ *with probability* $p_1 = (p_{11}, \ldots, p_{1J})$*, and* $(s_{21}, \ldots, s_{2K})$ *with probability* $p_2 = (p_{21}, \ldots, p_{2K})$*, the expected payoff for the players are computed as follows:*

$$v_1(p_1, p_2) = \sum_{j=1}^{J} p_{1j} \left[\sum_{k=1}^{K} p_{2k} u_1(s_{1j}, s_{2k}) \right] = \sum_{j=1}^{J} \sum_{k=1}^{K} p_{1j} \cdot p_{2k} u_1(s_{1j}, s_{2k})$$

$$v_2(p_1, p_2) = \sum_{k=1}^{K} p_{2k} \left[\sum_{j=1}^{J} p_{1j} u_2(s_{1j}, s_{2k}) \right] = \sum_{j=1}^{J} \sum_{k=1}^{K} p_{1j} \cdot p_{2k} u_2(s_{1j}, s_{2k})$$

The mixed strategies (p_1^*, p_2^*) *are a Nash Equilibrium only if the mixed strategy for each player is the best response to the mixed strategy of the other player:*

$$v_1(p_1^*, p_2^*) \geq v_1(p_1, p_2^*) \text{ for any } p_1$$

$$v_2(p_1^*, p_2^*) \geq v_2(p_1^*, p_2) \text{ for any } p_2.$$

By applying Definition 4 we can now compute the Nash Equilibrium when the defender and the attacker adopt mixed strategies(Figure 4).

The utility of the defender u_d and of the attacker u_a are respectively:

$$u_d = 1p_{c_1}p_{a_1} + 1p_{c_1}p_{a_2} + 1p_{c_2}p_{a_1} + 1p_{c_3}p_{a_2}$$

$$u_a = 1p_{c_1}p_{a_1} + 1p_{c_2}p_{a_1} + 2p_{c_2}p_{a_2} + 2p_{c_3}p_{a_1} + 2p_{c_3}p_{a_2}.$$

Figure 5 shows an equilibrium with mixed strategy for the game: the defender plays the strategy c_1 with probability $\frac{1}{2}$ and c_2 with probability $\frac{1}{2}$, the attacker plays a_1 with probability 1.

		1 a_1	a_2
$\frac{1}{2}$	c_1	1,1	1,0
$\frac{1}{2}$	c_2	1,1	0,2
	c_3	0,2	1,2

Fig. 5. Example of mixed strategy.

4 Using economic indexes as payoffs

In this section we show how to model a security problem by using the results highlighted in the previous section. An enterprise's server is used to store information about customers. Consider the defense tree depicted in Fig. 6 reflecting attacks to the server (the asset) and the corresponding mitigation countermeasures.

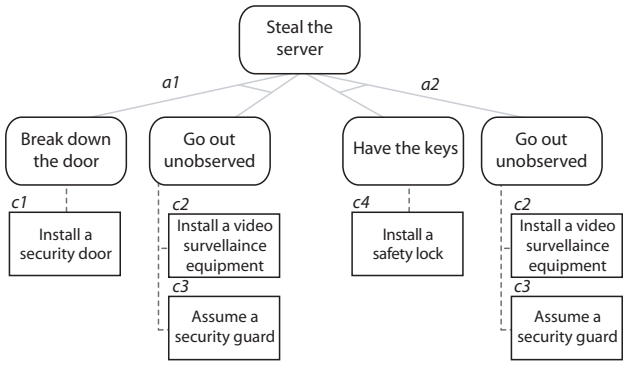


Fig. 6. Example of defense tree: theft of a server.

In the example we consider a server with a value of 100.000 €. The Exposure Factor (EF) and the Annualized Rate of Occurrence (ARO) of each attack are shown in Table 1. Notice that associated to the risk management process is the lack of reliable statistical data to use in a quantitative analysis. In our paper we use (when available) statistics collected in [12] that combine the information from two surveys: a magazine survey in Information Week (October 1996) that asked "What Security Problems have resulted in financial losses?", and another magazine survey, in InfoSecurity News May 1997 that asked "In the past 12 months, which of the following breaches have you experienced?".

We need now to compute ALE for each of the possible attacks. Considering the first attack of Figure 6 we can notice that for a successful attack we need

Attack	EF	ARO	Countermeasures	RM	CSI	ROI
a1 Break down the door and go out unobserved	90%	0,1	*c1* Install a security door	0,7	1500	3.20
			c2 Install a video surveillance equip.	0,1	3000	-0.70
			c3 Employ a security guard	0,5	12000	-0.63
			c4 Install a security lock	0	300	-1
a2 Open the door with keys and go out unobserved	93%	0,1	*c1* Install a security door	0	1500	-1
			c2 Install a video surveillance equip.	0,1	3000	-0.69
			c3 Employ a security guard	0,5	12000	-0.61
			c4 Install a security lock	0,2	300	5.20

Table 1. Computation of ROI.

Attack	Cost_a	Countermeasures	Cost_{ac}	ROA
a1 Break down the door and go out unobserved	4000	*c1* Install a security door	2000	0.50
		c2 Install a video surveillance equipment	1000	4.40
		c3 Employ a security guard	1500	1.73
		c4 Install a security lock	0	6.50
a2 Open the door with keys and go out unobserved	4200	*c1* Install a security door	0	6.14
		c2 Install a video surveillance equipment	1000	4.19
		c3 Employ a security guard	1500	1.63
		c4 Install a security lock	200	4.45

Table 2. Computation of ROA.

both to break down the door and to go out unobserved. So, the EF and ARO are associated to the pair of actions (and not to the leaf). We proceed similarly for the second attack.

The ALE associated to the attack are, respectively, ALE =100.000€×0.9 × 0.1 =9.000€ and ALE =100.000€×0.93 × 0.1 =9.300€.

The second step is to compute the ROI for each countermeasure by considering the cost (CSI) and the amount of risk mitigated (RM) of Table 1.Notice that the countermeasures c_1 and c_4 have two different RM values: in Figure 6 we can see that c_1 is used only to mitigate the attack a_1 in this case the value of RM is 0.7, but if it is used to mitigate the attack a_2 the value of decreases to 0. The same is true for the countermeasure c_4, if it is used to mitigate the attack a_2 the value of RM is 0.2 but if it is used for the attack a_1 RM is 0.

For the first countermeasure (installing a security door to mitigate the threat of breaking down a door), we have $ROI = \frac{(ALE \times RM) - CSI}{CSI} = \frac{(9.000€ \times 0.7) - 1.500€}{1.500€} = 3.20$. Similarly we can compute the ROI for all the other countermeasure as shown in Table 1.

For ROA we analyze the scenario from the attacker perspective. Let us suppose that the attacker has an advantage that can be economically quantified as 30.000€ for a successful attack to the server. By using the data in Table 2 we compute the ROA for each countermeasure.

Notice that the cost an attacker has to pay depends on the attack and on the countermeasure installed. In Table 2, for instance, the fixed cost to be sustained by the attacker from stealing the server is different (4.000 € or 4.200 €): the variable costs instead depends on the specific countermeasure (2.000 € when encountering a security door vs 1.000 € for a video surveillance installation).

The data in the table are used to compute ROA for all the countermeasures in the tree. So, for instance when installing a security door we can obtain a $ROA = \frac{GI \times (1-RM) - (cost_a + cost_{ac})}{cost_a + cost_{ac}} = \frac{30.000 € \times (1-0.7) - (4.000 € + 2.000 €)}{4.000 € + 2.000 €} = 0.50$. In a similar manner we can compute ROA for all the other countermeasures as shown in Table 2.

The resulting defense tree labeled with ROI and ROA for each countermeasure and attack is depicted in Figure 7.

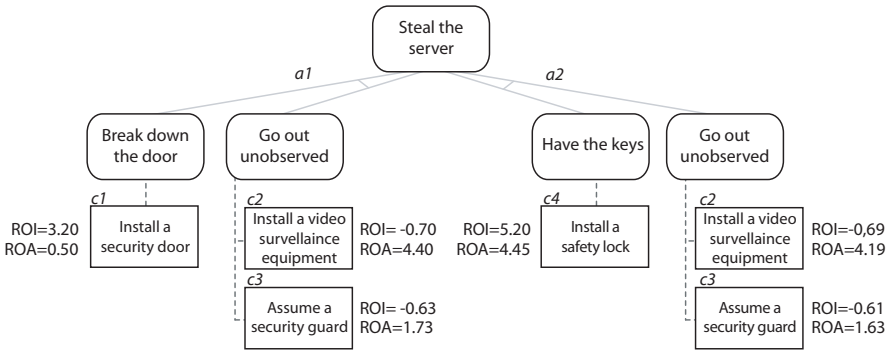


Fig. 7. The defense tree of Fig. 6 decorated with ROIs and ROAs.

4.1 Selection of a single countermeasure/attack

To model the defense tree as a strategic game we consider the set of strategies for the defender as composed by single countermeasures as represented in Figure 6. In a similar manner the strategies for the attacker are just a_1 (the left hand side of the tree) and a_2 (the right hand side). The utility functions are the indexes ROI and ROA introduced in Section 2 as described in the bimatrix of Figure 8.

Now, using Definition 1, we look for a Nash Equilibrium of the game.
From the attacker's viewpoint: if the defender plays the strategy c_1 the best response of the attacker is to play the strategy a_2, if he plays strategies c_2, c_3 or c_4 the best response is strategy a_1. Instead, from the defender's viewpoint: if the attacker plays strategy a_1 the defender's best response is to play c_1, while if she plays a_2 or a_3 the defender plays c_4.

As consequence there are no Nash Equilibrium with pure strategies. In fact, our game is similar to a constant sum game where the payoffs of the two players have opposite rewards. The absence of so-called equilibrium points or saddle

	$a1$	$a2$
$c1$	3.20,0.50	-1.00,6.14
$c2$	-0.70,4.40	-0.69,4.19
$c3$	-0.63,1.73	-0.61,1.63
$c4$	-1.00,6.50	5.20,4.45

Fig. 8. Bimatrix for the attacker/defender game with single selection of countermeasures/attacks.

points (optimal for all players at once) means that there are no optimal situations in the sense that they provide to each participant the maximum of what he/she can get given the acts of the other players.

So there are no stable strategies to follow for the defender and the attacker in the game. In spite of the absence of a rational choice (some advice can be however given following other approaches [1]), when the game is repeated many times, some optimal lines of behavior can be found. To find them one must extend the analysis to include the adoption of mixed strategies by the players. As the criterion for the choice of optimal mixed strategies one takes the mathematical expectation value of the payoff which shows how much one can win on average by repeating the game many times.

Using Definition 4 (and Gambit [11], a tool for computing equilibria[4]) we look for mixed strategy equilibria.

The result is that there is one equilibrium if the defender plays the strategy c_1 with probability $\frac{205}{769}$ and c_4 with probability $\frac{564}{769}$, and if the attacker plays the strategy a_1 with probability $\frac{31}{52}$ and a_2 with probability $\frac{21}{52}$. We see that the probability for the two attacks are pretty close, so the system administrator cannot consider to reduce the attention to only one of the two branches. Moreover, it seems that the best that a system administrator can do is to invest in the countermeasure c_1 to avoid the first attack *and* in the countermeasure c_4 to avoid the second attack.

Notice however that this strategy is not so natural; in fact, why not to invest in countermeasure c_3 to be able to partially cover both the attacks? In the example studied here we do not study indeed the possibility to have both the attacks occurring simultaneously and to have more then one countermeasure implemented.

4.2 Selection of set of countermeasures/attacks

In the previous strategic game we considered only one attack/countermeasure strategy by each players. Here, instead, each player can play any set of countermeasures/attacks together (but we have also the possibility to select no attack or countermeasure).

In order to avoid some technical problems (division by 0) when dealing with empty sets of countermeasures or attacks we change the utility functions for the

[4] Available at `http://econweb.tamu.edu/gambit/`.

two players. We retain the numerator from the old utility functions.

$$u_d = ALE \times RM - CSI$$
$$u_a = GI \times (1 - RM) - (cost_a + cost_{ac})$$

Using the new utility functions we obtain the strategic game of Figure 9.

	$\emptyset$	a1	a2	{a1,a2}
$\emptyset$	0, 0	0, 26.000	0, 25.800	0, 21.800
c1	-1.500, 0	4.800, 3.000	-1.500, 25.800	11.310, -1.200
c2	-3.000, 0	-2.100, 22.000	-2.070, 21.800	-1.170, 17.800
c3	-12.000, 0	-7.500, 9.500	-7.350, 9.300	-2.850, 5.300
c4	-300, 0	-300, 26.000	1.560, 19.600	3.360, 15.500
{c1,c2}	-4.500, 0	1.800, 2.000	-3.570, 21.800	8.310, -2.200
{c1,c3}	-13.500, 0	-7.200, 1.500	-8.850, 9.300	-690, -2.700
{c1,c4}	-1.800, 0	4.500, 3.000	60, 18.600	11.010, -1.500
{c2,c3}	-15.000, 0	-10.500, 8.500	-10.350, 8.300	-5.850, 4.300
{c2,c4}	-3.300, 0	-2.400, 22.000	-1.440, 18.600	360, 14.500
{c3,c4}	-12.300, 0	-7.800, 9.500	-7.650, 9.100	-3.150, 5.000
{c1,c2,c3}	-16.500, 0	-10.200, 500	-11.850, 8.300	-3.690, -3.700
{c1,c2,c4}	-4.800, 0	1.500, 2.000	-2.940, 18.600	8.010, -2.500
{c1,c3,c4}	-13.800, 0	-7.500, 1.500	-9.150, 9.100	-990, -3.000
{c2,c3,c4}	-15.300, 0	-10.800, 8.500	-10.650, 8.100	-6.150, 4.000
{c1,c2,c3,c4}	-16.800, 0	-10.500, 500	-12.150, 8.100	-3.990, -4.000

Fig. 9. Bimatrix for the attacker/defender game with a set selection of countermeasures/attacks.

Once again there are no Nash Equilibria with pure strategy, but Gambit computes a mixed equilibrium where the defender plays the strategy c_4 with probability $\frac{39}{55}$ and $\{c_1, c_4\}$ with probability $\frac{16}{55}$, and the attacker plays the strategy a_1 with probability $\frac{5}{21}$ and a_2 with probability $\frac{16}{21}$.

As a side result we note that two compound strategies by the attacker, namely $\emptyset$ and $\{a_1, a_2\}$, are uniformly dominated by the simple strategies a_1 and a_2. This shows that the attacker has no interest in combining the actions together.

5 Conclusions and Future Work

The use of game theory, allow us to model the interaction between the attacker and the defender: they represent two players with opposite goals. The tactical choices of each one of the player strictly depends from the moves of the other. In particular, when an attacker has to select a possible attack for an asset, he/she has to consider necessarily the possible countermeasure that the defender have introduced into the system; vice-versa, when a system administrator has to select which countermeasure introduce in order to protect the system, he has to consider the possible attacks that the attacker could perform.

Using the Nash Equilibria allow us to model the above situation where attacker and defender need to take some decision. The Nash equilibrium has been used [10][5] to determine the best move of the two players, by considering the fix point of the interactions between attacker and defender.

In this paper we first, used defense trees as extension of attack trees with countermeasures and economic quantitative indexes for modeling attack scenarios. Then such scenarios are analyzed as strategic games. The strategies of the two players (the defender can select countermeasures and the attacker can choose among several vulnerabilities to exploit) lead to different payoffs represented as economic indexes. In particular ROI and ROA are used. The study confirms that investments beyond a certain level do not produce any beneficial effect after a certain point are not anymore useful [7] (so, only a subset of the countermeasure usually has to be considered).

The methodology presented in this paper provides a basis for future work along several research directions.

While it may seem obvious to compute the solution cost of a set $C = \{c_1, c_2\}$ of countermeasures as the sum $CSI_C = CSI_{c_1} + CSI_{c_2}$ of the costs of the single countermeasures in C, it should be noticed that the total cost of implementing a set of countermeasures could realistically be less than CSI_C (e.g. discounted price of bundled security solutions) or greater than CSI_C (e.g. when countermeasures must be managed by different employees, due to the existence of separation of duty constraints [2]).

On the other hand, it is not clear how to compute the value of the Risk Mitigated attribute for a set of countermeasures $\{c_1, c_2\}$, as any value between $\max(RM_{c_1}, RM_{c_2})$ (one countermeasure strictly entails the other) and $(RM_{c_1} + RM_{c_2})$ (completely independent countermeasures) appears to be acceptable depending on the type and nature of countermeasures and the asset being protected.

We plan to extend this work by considering n player games (where we have 1 defender and $n-1$ attackers). This could lead to interesting discussion about the amount of cooperation between the attacker. Usually attackers try to cooperate, unless the cooperation reduces their gain too much (that is, the benefit coming from the attack has to be divided among them).

When considering several attackers also notions of *types* (and bayesian games) could be important. From which type of attacker we expect to have the attack? We can differentiate between attacker w.r.t. their propension/aversion to risk?

Dynamic games provide another source for extension. Repeat games with the normal games described above as a stage game could be considered. As well a game when both players refine their information as the sequence of attacks and countermeasures progress.

We hope our work can help encourage research and experimentation with the use of economic indexes and combined development of attacker/defender perspectives during evaluation of alternative security investments.

References

1. Stefano Bistarelli, Fabio Fioravanti, and Pamela Peretti. Defense tree for economic evaluations of security investment. In *1st International Conference on Availability, Reliability and Security (ARES'06)*, pages 416–423, 2006.
2. D.D. Clark and D.R. Wilson. A comparison of commercial and military computer security policies. In *In IEEE Symposium on Computer Security and Privacy*, 1987.
3. Marco Cremonini and Patrizia Martini. Evaluating information security investments from attackers perspective: the Return-On-Attack (ROA). In *Fourth Workshop on the Economics of Information Security*, June 2005.
4. Nathalie Louise Foster. *The application of software and safety engineering techniques to security protocol development*. PhD thesis, University of York, Department of Computer Science, 2002.
5. D. Fudenberg and J. Tirole. *Game Theory*. MIT Press, 1991.
6. Robert Gibbons. *A Primer in Game Theory*. Pearson Higher Education, 1992.
7. Lawrence A. Gordon and Martin P. Loeb. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.*, 5(4):438–457, 2002.
8. Howard and LeBlanc. *Writing Secure Code*. Microsoft Press, 2002.
9. Ronal L. Krutz, Russell Dean Vines, and Edward M. Stroz. *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security*. Wiley, August 2001.
10. Yu Liu. *Intrusion Detection for Wireless Networks*. PhD thesis, Stevens Institute of Technology, 2006.
11. Richard D McKelvey, Andrew M. McLennan, and Theodore L. Turocy. Gambit: Software tools for game theory (version 0.2006.01.20), 2006. http://econweb.tamu.edu/gambit.
12. James W. Meritt. A method for quantitative risk analysis. In *Proceedings of the 22nd National Information Systems Security Conference*, October 1999.
13. Martin J. Osborne. *An introduction to game theory*. Oxford Univ. Press, 2003.
14. Stuart E. Schechter. *Computer Security Strength & Risk: A Quantitative Approach*. PhD thesis, Harvard University, May 2004.
15. Bruce Schneier. Attack trees: Modeling security threats. Dr. Dobb's Journal, 1999.
16. Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000.
17. Wes Sonnenreich, Jason Albanese, and Bruce 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*, pages 239–252. INSTICC Press, 2005.
18. Gary Stoneburner, Alice Goguen, and Alexis Feringa. Risk management guide for information technology systems. Nist special publication 800–30, NIST, National Institute of Standard Technology, July 2002.