Security Analysis Using Subjective Attack Trees

Nasser Al-Hadhrami[0000−0003−2484−7444], Matthew Collinson[0000−0002−0496−2990], and Nir Oren[0000−0002−4854−9014]

University of Aberdeen, AB24 3UE, Aberdeen, UK
{r01nama,matthew.collinson,n.oren}@abdn.ac.uk

Abstract. Subjective attack trees are an extension to traditional attack trees, proposed so to take uncertainty about likelihoods of security events into account during the modelling of security risk scenarios, using subjective opinions. This paper extends the work of subjective attack trees by allowing for the modelling of countermeasures, as well as conducting a comprehensive security and security investment analysis, such as risk measuring and analysis of profitable security investments. Our approach is evaluated against traditional attack trees. The results demonstrate the importance and advantage of taking uncertainty about probabilities into account. In terms of security investment, our approach seems to be more inclined to protect systems in presence of uncertainty (or lack of knowledge) about security events evaluations.

Keywords: Attack trees · Risk analysis · Subjective logic.

1 Introduction

In [1], we defined a new model of attack trees (ATs), called a Subjective Attack Tree (SAT), that takes uncertainty about likelihoods of successful attacks (in literature, also referred to as security events) into account. The SAT model aims to address the limitations of traditional probabilistic attack trees [6, 14, 15], which use precise values for likelihoods of security events. In many situations, it is difficult to elicit accurate probabilities due to lack of knowledge, or insufficient historical data, making the evaluation of risk in existing approaches unreliable. The SAT model allows for *uncertainty* modelling about likelihoods, via *subjective opinions* in the formalism of Subjective Logic [9]. We also discussed how subjective opinions are propagated in the model, via the gates of AND and OR, to compute a subjective opinion on the root node.

The work in [1], however, still lacks several important components for a useful and effective risk and decision analysis. A comprehensive security analysis requires, in addition to likelihoods of attacks, additional metrics such as cost of attack, impact, cost of security investments, etc. Several works have considered the formalism of defense tress, models that add defense mechanisms (i.e., countermeasures) to ATs, e.g. [8, 12, 16]. These models make use of such metrics to conduct a complete security and risk analysis, and study the efficacy of proposed countermeasures using economic terms such as Return on Investment

(ROI) and Return on Attack (ROA) [2, 17]. Any security or security investment analysis makes use, as an essential component, of probabilistic values. Since likelihoods in the SAT model are subjective opinions, it is essential to discuss how security or security investment analysis is conducted, showing at the same time how to handle uncertainties in the model for an effective decision analysis.

In this paper, we extend the SAT model by allowing for the conducting of a comprehensive analysis of security (e.g., risk measuring) and security investment with ROI index to determine which countermeasures are more profitable. This paper thus makes the following contributions. (1) we discuss the adding of countermeasures to the SAT model, and how these countermeasures reduce risk in presence of uncertainty about probabilities. (2) we conduct security and decision analysis, including risk computation, and security investment analysis using ROI index. (3) we conduct an experimental evaluation that compares the security and investment analysis in SATs with the one in traditional ATs.

In Section 2, we give an overview of subjective logic, followed by an overview of the SAT model in Section 3. In Section 4, we discuss the adding of countermeasures to SAT model. In Section 5, we discuss security and security investment analysis in SATs. In Section 6, we demonstrate the usability of our approach in the context of security analysis using the scenario of DDoS attack. In Section 7, we evaluate our approach against traditional ATs. Finally, in Section 8, we conclude the paper, discussing prospects for future work.

2 Subjective Logic

Subjective logic [9] is a formalism for reasoning under uncertainty that extends probabilistic logic by allowing also for uncertainty degrees to be expressed about probability values, via subjective opinions. In subjective sogic [9], a subjective opinion represents the probability distribution of a random variable complemented by an *uncertainty* degree about the distribution. Let us assume a proposition X such as *the workstation is compromised*. The validity of X is uncertain in general, but we can assume there is a "ground truth" probability p_x that X is *true*, and $p_{\bar{x}}$ (i.e., $1 - p_x$) that X is *false*. This makes X a binary random variable over the domain $\mathbb{X} = \{x, \bar{x}\}$. Little amount of evidence supporting this proposition, or a lack of relevant knowledge, will affect giving the exact probabilities p_x and $p_{\bar{x}}$. As such, the analyst needs to give a subjective opinion about them, expressed in terms of *beliefs* and *uncertainty*.

A subjective opinion on a binary random variable X, called a *binomial opinion*, is a tuple $\omega_X = \langle b_x, d_x, u_x, a_x \rangle$, representing the *belief*, *disbelief* and *uncertainty* that X is true at a given instance, and a_x is the *prior* probability (also called the base rate) that X is true in the absence of observations. A *prior weight* $W > 0$ is defined indicating the strength of the prior assumption. An opinion's parameters must satisfy: a) $b_x, d_x, u_x, a_x \in [0, 1]$, and b) $b_x + d_x + u_x = 1$. For a given binomial opinion ω_X, the corresponding *projected probability distribution* $\mathbf{P}(x) : x \rightarrow [0, 1]$ is determined as $\mathbf{P}(x) = b_x + a_x \cdot u_x$, where $\mathbf{P}(x)$ represents the probability estimation of x which varies from the base rate value, in the case of complete ignorance ($u_x = 1$), to the actual probability in case that $u_x = 0$.

A binomial opinion translates directly into a Beta distribution. The value of a Beta-distributed random variable X is determined from N_{ins} independent observations. Let $n_x, n_{\bar{x}}$ be the total number of observations supporting $X = x$ and $X = \bar{x}$ respectively. Then the Beta parameters $\alpha_X = \big\langle n_x + Wa_x, n_{\bar{x}} + W(1-a_x)\big\rangle$, where a_x is the prior assumption, and W is a prior weight indicating the strength of the prior assumption. Unless specified otherwise, we assume $a_x = 0.5$, and $W = 2$, yielding a uniform distribution for the prior assumption.

Given a subjective opinion $\omega_X = \big\langle b_x, d_x, u_x, a_x\big\rangle$, we compute the corresponding Beta parameters $\alpha_X = \big\langle \alpha_x, \alpha_{\bar{x}}\big\rangle$ as $\alpha_X = \Big\langle \frac{W}{u_x} b_x + Wa_x, \frac{W}{u_x} dx + W(1-a_x)\Big\rangle$. Conversely, given Beta parameters $\alpha_X = \big\langle \alpha_x, \alpha_{\bar{x}}\big\rangle$, a transformation from the Beta distribution to a subjective opinion is given as $\omega_X = \Big\langle \frac{\alpha_x - Wa_x}{S_X}, \frac{\alpha_{\bar{x}} - W(1-a_x)}{S_X}, \frac{W}{S_X}, a_x\Big\rangle$. where S_X is the *Dirichlet strength* of the beta distribution. Equations for computing the Dirichlet strength, mean, and variance directly from a subjective opinion are discussed in [4].

3 An Overview of Subjective Attack Trees

A Subjective Attack Tree (SAT) [1] is an extension to traditional attack trees, proposed so to take uncertainty about likelihoods of security events into account during the modelling of security risk scenarios, via subjective opinions. Fig 1 shows an example SAT with three possible paths (ways) an attacker can choose to achieve their main goal (MG). These paths begin by the execution of the following security events: (SE_1 and SE_2), SE_3, and (SE_4 and SE_5). Taking the first path with security events SE_1 and SE_2 as an example, the subjective opinions on them, respectively, are denoted by ω_{SE_1} and ω_{SE_2}. The subjective opinion on sub-goal 1 (ω_{SG_1}) is computed from the *conjunction* of ω_{SE_1} and ω_{SE_2}, and the subjective opinion on the main goal (ω_{MG}) is computed from the *disjunction* of ω_{SG_1} and ω_{SG_2}. The subjective opinion on MG represents the *belief* that an attacker can successfully achieve their main goal, the *disbelief* that an attacker can successfully achieve their main goal, and the *uncertainty* degree about the distribution of these belief and disbelief masses.

In SAT model, subjective opinions are propagated through AND gate using the *conjunction* operator of subjective logic [9], and the *disjunction* operator in case of OR gate. Fig 2 (b) shows an example computation of a subjective opinion on event Z via OR gate.

4 Adding Countermeasures to SATs

The SAT model does not take into account defense mechanisms that can be implemented by the defending organization and the costs sustained for security investments. We discuss the adding of countermeasures to the SAT model with

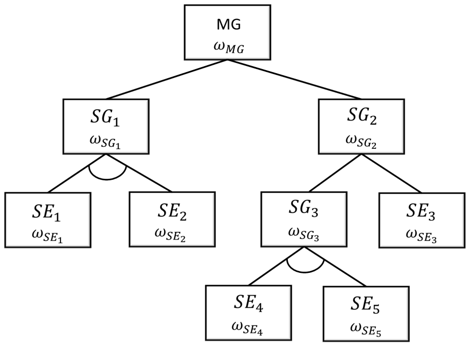
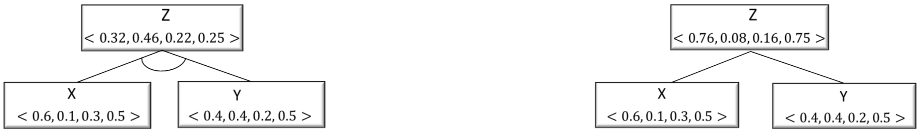


Fig. 1: A Subjective Attack Tree (SAT) model.



(a) (b)

Fig. 2: Computing an opinion on event Z via (a) AND gate, and (b) OR gate.

the aim to reduce risk (i.e., likelihood of successful attacks). Countermeasures in our approach can be placed at any node in the tree as per the approach in [16]. Adding countermeasures to ATs models in general is aimed to minimise the likelihood of attacks. In the SAT model, the likelihoods are subjective opinions, so we discuss how these opinions are affected when adding countermeasures.

Each added countermeasure should be associated a value representing the effectiveness of the countermeasures in reducing risk. In most existing approaches, the effectiveness value of a countermeasure is expressed as a percentage, and the likelihood of an attack in presence of the countermeasure is then calculated by multiplying the likelihood value with the given percentage for the countermeasure's effectiveness. However, when there is uncertainty about the likelihood (as in SATs), the calculation would differ. In SATs, adding a countermeasure does not reduce the uncertainty about the likelihood of an event, but the belief mass and base rate. Therefore, the effectiveness value will affect only the belief mass and base rate while maintaining the same uncertainty value. The disbelief mass is calculated by subtracting the total value of the resulting new belief mass and uncertainty from one. Formally, assuming $\omega_{SE} = \langle b_{se}, d_{se}, u_{se}, a_{se} \rangle$ is the subjective opinion about a security event SE, C a potential countermeasure to reduce risk, and CE the countermeasure effectiveness. We compute the opinion about SE with countermeasure C, denoted by $\omega^{'}_{SE} = \langle b^{'}_{se}, d^{'}_{se}, u^{'}_{se}, a^{'}_{se} \rangle$, as follows

1. $b^{'}_{se} = b_{se} \times (1 - CE)$
2. $a^{'}_{se} = a_{se} \times (1 - CE)$
3. $u^{'}_{se} = u_{se}$

4. $d'_{se} = 1 - (b'_{se} + u'_{se})$

Fig 3 shows an example SAT model with two applied countermeasures (ovals), and how they reduce risk according to the above discussion.

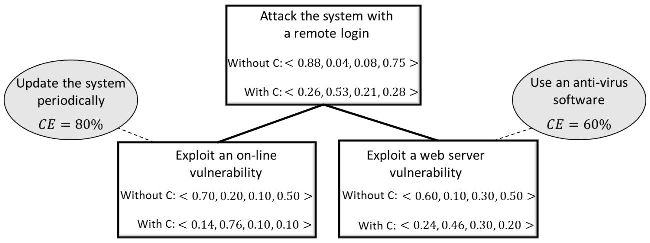

Attack the system with a remote login
Without C: < 0.88, 0.04, 0.08, 0.75 >
With C: < 0.26, 0.53, 0.21, 0.28 >
Update the system periodically
CE = 80%
Use an anti-virus software
CE = 60%
Exploit an on-line vulnerability
Without C: < 0.70, 0.20, 0.10, 0.50 >
With C: < 0.14, 0.76, 0.10, 0.10 >
Exploit a web server vulnerability
Without C: < 0.60, 0.10, 0.30, 0.50 >
With C: < 0.24, 0.46, 0.30, 0.20 >

Fig. 3: A SAT model with two countermeasures (ovals), showing how they reduce likelihoods (i.e., opinions) on the leaves, and subsequently on the root node.

5 Security Analysis in SATs

5.1 Risk Computation

In the context of risk analysis, risk is typically computed using the well-known formula *risk* = *probability* × *impact*. In ATs, the computation of risk is often done at the root node (i.e., risk caused by the successful achievement of the attacker's goal). In SATs, we deal with subjective opinions rather than probabilities, and so the risk calculation is different. Risk calculation in SATs depends basically on how the impact value was represented. In literature , most existing approaches represent impact as single values within the interval [0, 1], and very rare is represented as a beta distribution, e.g., [13] for characterizing earthquake damage. In this paper, we demonstrate how risk is computed in case that the impact is a single value and in case is given as a beta distribution.

In contrast to the traditional one, risk calculation in our approach results in a distribution of risk (loss) values in the form of a beta distribution. This is because that there is an uncertainty distribution about the likelihood, expressed in subjective opinions, and these opinions, as discussed in Section 2, have one-to-one correspondence to beta distributions. The loss distribution is therefore a beta distribution, provided that the impact value belongs to the interval [0, 1].

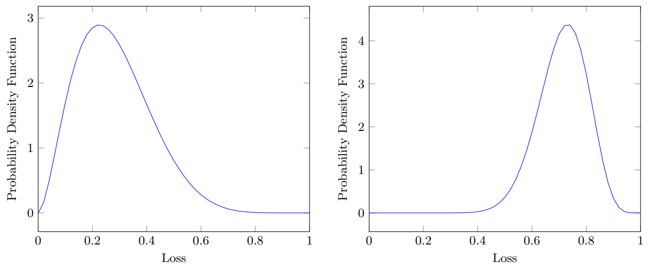
Risk computation with a single value of impact: when the impact is given as a single value within the interval [0, 1], risk is calculated as follows. First, we multiply the projected probability of the subjective opinion (see Eq 2) with the impact value to obtain the mean of risk, R_μ. Second, we compute the Dirichlet strength of the subjective opinion (see [4]), as this would represent also the Dirichlet strength of risk S_R. Having R_μ and S_R, we can compute the Beta parameters of risk as follows: $\alpha = \langle R_\mu . S_R, (1 - R_\mu) . S_R \rangle$.

Example 1. Suppose the subjective opinion about security event SE is $\omega_{SE} = \langle 0.6, 0.2, 0.2, 0.5 \rangle$, and the impact is 0.4. The mean of risk $R_\mu = 0.7 \times 0.4 = 0.28$, where 0.7 is the projected probability of ω_{SE}. The Dirichlet strength of ω_{SE} is 10, and so $S_R = 10$. Accordingly, $\alpha = \langle 0.28 \times 10, (1 - 0.28) \times 10 \rangle = \langle 2.8, 7.2 \rangle$. The beta distribution of risk in this example is shown in Fig 4 (a).

Risk computation with a beta distribution representation of impact: when the impact is given as a beta distribution, we compute risk as follows:

1. we translate the given subjective opinion into the corresponding beta distribution, and then compute its mean and variance.
2. we compute the mean and variance of the impact from the given beta parameters of the impact distribution.
3. we use the product operator of independent Beta-distributed random variables (see [4]) to compute the mean and variance of risk.
4. we use these mean and variance of risk to compute its beta parameters.

Example 2. Suppose an opinion about event SE is $\omega_{SE} = \langle 0.9, 0.0, 0.1, 0.5 \rangle$. Suppose also the impact I is represented as a beta distribution with shape parameters $\alpha = \langle 18, 4 \rangle$. The risk distribution is then obtained by first computing the mean and variance of both the likelihood (ω_{SE}) and impact distributions. This yields $\mu_{SE} = 0.95$, $\sigma^2_{SE} = 0.00226$, $\mu_I = 0.75$, and $\sigma^2_I = 0.0075$. Using the product operator [4], we obtain the mean and variance of risk R as $\mu_R = 0.7125$ and $\sigma^2_R = 0.0.00805$. Using these values, we obtain beta parameters for risk as $\alpha = \langle 17.41, 7.03 \rangle$. The risk distribution is shown in Fig 4 (b).



(a) (b)

Fig. 4: The beta distributions of loss (risk) in (a) Example 1 and (b) Example 2, where ”0” indicates no risk and ”1” the risk is catastrophic.

Since both representation of impact (the single value and beta distribution representation) yields a beta distribution for risk, for simplicity, in the rest of the paper, we model impact as single values. Our approach of decision analysis takes into account the uncertainty about a likelihood or about risk, so we discuss in the next section, how we deal with uncertainty for risk and decision analysis.

5.2 Dealing with Uncertainty for Decision Analysis

In our approach, metrics such as likelihood and risk are defined as beta distributions (given that subjective opinions, for likelihoods, can be translated into the corresponding beta distributions) rather than single values. For decision analysis, it is important to handle the uncertainty in such metrics, as we will see in the next section. We discuss in this section two possible approaches to reason about risk (or likelihood) in presence of uncertainty. These approaches are (1) reasoning with the most expected value, and (2) reasoning with best and worst-case scenarios via confidence intervals.

Approach 1: Reasoning with the Most Expected Value: In this approach, security managers use the most expected value about a likelihood (or risk) for decision-making. In case of likelihood, the most expected value is the projected probability of the subjective opinion, and it is the mean in case of the risk distribution. This approach yields a single value of risk, and therefore the decision analysis would be similar to the traditional approaches of risk assessment, except that in our approach the uncertainty value is taken into account when computing the most expected value.

Approach 2: Reasoning with Confidence Intervals for Best and Worst-Case Scenarios: In this approach, risk is represented by a range of possible values, determined by lower and upper bounds with a given confidence level, rather than single values, allowing for best- and worst-case scenarios to be considered. In literature, several approaches exist to compute confidence intervals of a beta distribution, e.g., [5, 10]. A simple approach is the one discussed in [11], wherein the lower bound of the confidence interval is determined as $1 - BETAINV(1 - \alpha/2, n - k + 1, k)$, and the upper bound as $BETAINV(1-\alpha/2, k+1, n-k)$, where α is the level of statistical significance, k the number of events observed, and n the sample size. $BETAINV()$ is the cumulative distribution function of a beta distribution. The lower and upper bounds calculated from these two equations will determine the range of possible values that the risk value is likely to be within.

5.3 Analysing Security Investment: ROI Analysis

Return on investment (ROI) ([17]) is an economic metric that is widely used to measure the profit obtained by the implementation of a specific countermeasure CM_i (thereby evaluating the efficacy of an investment or comparing the efficacy of a number of different investments). ROI directly measures the amount of return on a particular investment, relative to the investment's cost. According to [17], ROI for a security investment is defined as

$$ROI = \frac{(\text{Risk exposure} \times \%\text{Risk mitigated}) - \text{Investment cost}}{\text{Investment cost}} \tag{1}$$

In AT models, *risk exposure* represents risk at the root node. Since countermeasures do not affect impact value directly (the impact value at the root node is the same apart from whether there were countermeasures applied or not), but rather the likelihood of an event occurrence [16], we may consider risk exposure as the *likelihood* (in SAT, the *subjective opinion*) about the goal (i.e., the top event) when we come to compute ROI. *% Risk mitigated* is the amount of the percentage risk mitigated as a result of applying a specific countermeasure. Unlike traditional probabilistic values, it is difficult to calculate directly such a percentage because the uncertainty value and base rate at the root node might change when applying a countermeasure to the model. Therefore, we have first to resolve uncertainty in the subjective opinions, using one of the approaches discussed in Section 5.2, to be able to compute the percentage risk mitigated, and use this percentage in the above ROI formula.

As an example, suppose the subjective opinion at the root node without countermeasure CM_i is $\omega_{goal_{-without-CM_i}} = \langle 0.65, 0.15, 0.20, 0.85\rangle$ and with the countermeasure is $\omega_{goal_{-with-CM_i}} = \langle 0.42, 0.25, 0.33, 0.72\rangle$. Suppose also we want to reason about risk using the most likely value, i.e., the projected probability of each subjective opinion. The projected probability of $\omega_{goal_{-without-CM_i}}$ is 0.82, and it is 0.66 for $\omega_{goal_{-with-CM_i}}$. The percentage risk mitigated is then calculated as $1 - \frac{0.66}{0.82} \times 100 = \%19.5$. For abbreviation,, we denote such a calculation for risk mitigated by RM.

Investment cost is the cost of the applied countermeasure. Based on the above discussion, we re-define ROI for a countermeasure CM_i as

$$ROI_{CM_i} = \frac{(R_{sys} \times \%RM) - C_{CM_i}}{C_{CM_i}} \tag{2}$$

where R_{sys} is the system risk, i.e., the opinion on the root node ω_{goal}, with an uncertainty treated according to the approaches in Section 5.2. In other words, R_{sys} can take any of the following values: the projected probability of ω_{goal}, the lower bound of the desired confidence interval, or its upper bound. A countermeasure CM_i is only profitable if $(R_{sys} \times \%RM) > C_{CM_i}$, and this is satisfied when the risk value is withing the scale of [0, 100] rather than [0, 1] ([3]). Therefore, we calculate risk as $R_{sys} \times 100$. If ROI is zero or a negative number, the investment is not profitable. Otherwise, it is financially justified, and so the higher value of ROI the higher desired an investment. Suppose in the given example above, the cost for implementing CM_i is \$20. ROI_{CM_i} is then $(82 \times 0.195) - 20)/20 = -0.2$. Since ROI is negative, the countermeasure is not profitable.

6 An Illustrative Example

To demonstrate the usability of our approach in security analysis, we use the example of DDoS attack discussed in [7] as a case study. To simplify the example, we show only portions of the complete scenario for implementing DDoS attack as depicted in Fig 5. The effectiveness of each countermeasure is shown in Fig 5, and their costs of implementation (in \$) are given as follows: $C(CM_1) = 10$, $C(CM_2) = 20$, $C(CM_3) = 15$, and $C(CM_4) = 20$.

Further, the model shows the impact values (below the subjective opinions). The propagation of impact values follows the approach in [15]. In case of OR gate, we choose to propagate the maximum value of impact to consider the worst-case scenario in calculating the impact at the root node. We do so because the analyst has to be prepared for the worst possible consequence (i.e., the attack with maximum impact) and because the attacker's capabilities and preferences cannot be known in advance. In case of AND gate, the impact values are propagated in the model according to formula defined in [8]. However, since our impact scale is [0, 1] and not [1, 10], we redefine the propagation rule of impact values as follows $1 - \prod_{i=1}^{n}(1 - I_{A_i})$, where n is the number of children nodes.

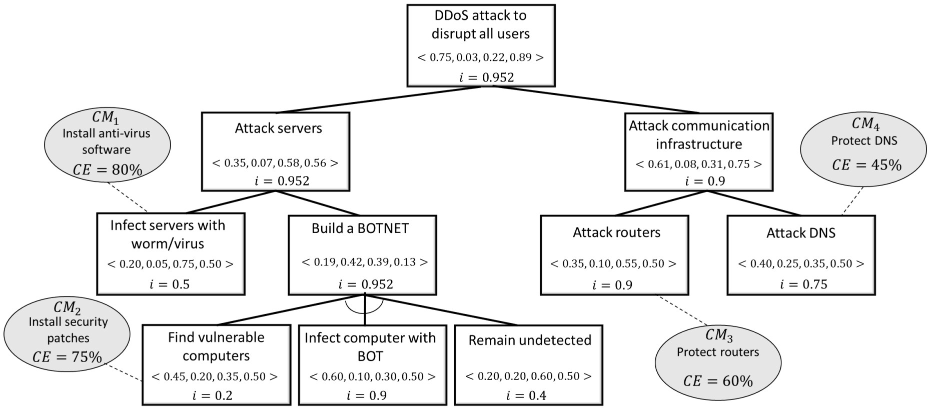


Fig. 5: The SAT model with countermeasures (ovals) for the DDoS attack scenario. The values below the subjective opinions are the impact values.

Table 1: The subjective opinion on the root node, risk mitigated, and ROI for each countermeasure in the DDoS attack scenario.

Applied countermeasure	Subjective opinion on goal	Risk mitigated	ROI
CM_1	$\langle 0.56, 0.13, 0.31, 0.72 \rangle$	18%	0.70
CM_2	$\langle 0.67, 0.09, 0.24, 0.81 \rangle$	09%	-0.57
CM_3	$\langle 0.61, 0.14, 0.25, 0.74 \rangle$	16%	0.01
CM_4	$\langle 0.68, 0.04, 0.28, 0.84 \rangle$	03%	-0.85

The subjective opinion about DDoS attack is $\langle 0.75, 0.03, 0.22, 0.89 \rangle$, and the impact is 0.952. Therefore, the risk is a beta distribution with parameters $\alpha = \langle 8.19, 1 \rangle$. The mean of risk is 0.9, representing the most likely value of risk. The 95% confidence interval of the risk distribution is [0.833, 0.967], representing the lowest and highest possible values. Security managers, unlike in traditional risk assessment approaches, can use these values to reason about risk and make decisions as per their risk attitudes.

We now turn our attention to the analysis of security investment, using ROI index. Applying each countermeasure would result in a reduction in the subjective opinion about the top event, i.e., ω_{goal}. Table 1 shows the subjective opinion about DDoS attack when applying each countermeasure, and the percentage risk mitigated after resolving uncertainty about the subjective opinions using the most likely value approach. Using Eq 2, we obtain ROI for each countermeasure as shown in Table 1. As appear, two countermeasures, CM_2 and CM_4, since their ROI are negative numbers, should be excluded. The only two countermeasures that are profitable are CM_1 and CM_3, and CM_1 is more profitable than CM_3. However, ROI for CM_3 approaches from zero, and so it does not seem to be significantly financially justified. As a result, the security manager may think of applying CM_1 (install anti-virus software) as a possible security solution against the DDoS attack.

7 Experimental Evaluation

We use the SAT model in Fig 6 as an example model to conduct an evaluation of our approach against traditional ATs in terms of security and security investment analysis. The model contains two countermeasures CM_1 and CM_2 applied to the security events SE_1 and SE_2, respectively. The subjective opinions about the four security events were established so as to contain relatively high uncertainty values. Propagating these opinions led to also a relatively high uncertainty (0.38) about the likelihood on the root node. The uncertainty values in the opinions lead to several different underlying probability values in contrast to a 0 uncertainty. For example, the probabilities of 0.75, 0.6, and 0.55 might represent possible truth values for the opinion about SE_4 ($\langle 0.40, 0.25, 0.35, 0, 50 \rangle$). In this example, the uncertainty value has affected only the belief mass of the

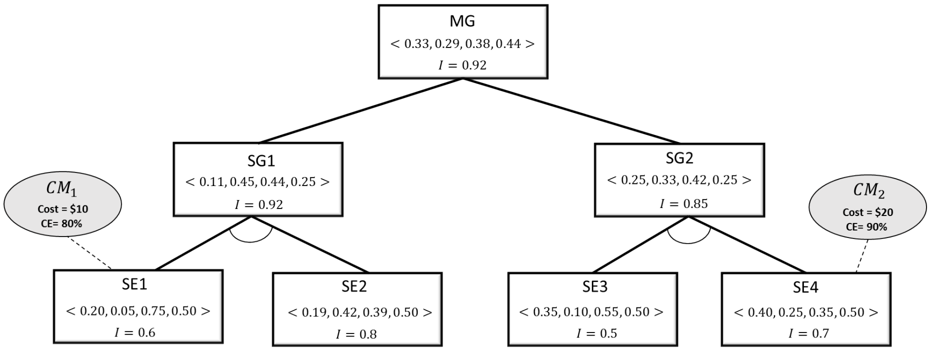


Fig. 6: A SAT model with two countermeasures. The values below the subjective opinions are impact values.

probability distribution of 0.75, affected only the disbelief mass of the probability distribution of 0.6, and affected both the belief and disbelief masses of the probability distributions of 0.55. Based on such a discussion, we generated probability values for the four security events (assuming they represent truth values) as follows: $Prob(SE_1) = 0.3$, $Prob(SE_2) = 0.25$, $Prob(SE_3) = 0.4$, and $Prob(SE_4) = 0.45$. Accordingly, the probability at the root node is 0.24.

First, we began by comparing the risk outcomes from the SAT model of Fig 6 with the risk obtained from applying traditional risk analysis using the above set of probabilities. In case of the SAT model, the risk obtained is a beta distribution with parameters $\alpha = \langle 4.6, 5.4 \rangle$ and mean 0.46. The 95% confidence interval of the risk distribution is [0.39, 0.52]. In case of the AT approach, the risk obtained is the single value 0.24. Suppose the security manager would only protect the system against the attack if the risk is greater than 0.45. It is evident that *in case of the AT approach, the system would not be protected. In case of the SAT model, there are cases in which the security manager would choose to protect the system.* If they rely on the most likely value (the mean of risk), or if the are too pessimistic and wish to consider the worst case scenario (via the upper bound of the confidence interval), they will go for protecting the system, since both values are greater than the defined threshold value. However, the decision would be the same as in the AT approach if they are optimistic and wish to consider the best case scenario (via the lower bound of the confidence interval).

Table 2: The projected probability of each subjective opinion about the attack with and without countermeasures and their 95% confidence interval.

Subjective opinion on attack	Projected probability	95% Confidence interval
$\langle 0.33, 0.09, 0.38, 0.44 \rangle$	0.5	[0.29, 0.71]
$\langle 0.27, 0.32, 0.41, 0.26 \rangle$	0.37	[0.12, 0.61]
$\langle 0.14, 0.44, 0.42, 0.27 \rangle$	0.25	[0.03, 0.47]

Next, we evaluated security investments (with ROI index) using the two approaches. In the SAT model, the subjective opinion about the attack without countermeasures is $\langle 0.33, 0.09, 0.38, 0.44 \rangle$. When applying each of CM_1 and CM_2 to the model, the resulting subjective opinions are $\langle 0.27, 0.32, 0.41, 0.26 \rangle$ and $\langle 0.14, 0.44, 0.42, 0.27 \rangle$, respectively. The projected probability of each subjective opinion and their 95% confidence intervals are given in Table 2. Using these information and cost of each countermeasure, we considered three scenarios to compute ROI for each countermeasure: (1) the most likely scenario (based on the projected probability), (2) the worst-case scenario (based on the lower bound of the confidence interval), and (3) the best-case scenario (based on the upper bound of the confidence interval). We denote the ROI calculated from the first scenario by ROI_{μ}, and by ROI_{lower} and ROI_{upper} for the other two scenarios, respectively. The ROI values obtained for each countermeasure are all positives (except in one case) as shown in Table 3.

Table 3: ROI values for each countermeasure in case of SAT model (ROI_μ, ROI_{lower}, and ROI_{upper}) and in case of AT approach (ROI_{pro}).

Countermeasure	ROI_μ	ROI_{lower}	ROI_{upper}	ROI_{pro}
CM_1	0.3	0.6	0	-0.49
CM_1	0.25	0.29	0.17	-0.24

In case of AT approach, the ROI obtained for each countermeasure, denoted by ROI_{pro}, is -0.49 for CM_1 and -0.24 for CM_2 (see Table 3). Clearly, none of the countermeasures are profitable, unlike in the SAT model, wherein the two countermeasures are financially justified in the three defined scenarios, except with the worst-case scenario for CM_1, in which ROI returned a 0 value.

Analysing the above results, our experiments clearly demonstrate the importance of taking uncertainty into account when conducting security analysis using models such as ATs, as doing so can lead to completely different security decisions. In terms of risk analysis, the SAT model offers a more flexible approach to decision-making by allowing to consider different scenarios (e.g., the best and worst-case scenarios), and so allowing security managers to take decisions based on, for instance, their risk attitudes, or the organisation' financial capabilities. In terms of security investments analysis (with ROI index), it seems that taking uncertainty into account results in higher ROI values for countermeasures (in contrast to a 0 uncertainty). This means that the chance to apply a countermeasure in the SAT model is higher, which could be also interpreted as follows: *our approach seems to be more inclined to protect systems in case of uncertainty (or lack of knowledge) about security events evaluations.*

8 Conclusions and Future Work

We extended a previous work on subjective attack trees by allowing for the modelling of countermeasures as well as conducting a comprehensive security and security investment analysis with ROI index. We showed how to calculate risk in SATs, and how to handle uncertainty for decision-making. Finally, we evaluated our approach against traditional attack trees, showing that SATs lead to different outcomes in contrast to ATs, and in terms of security investment, they seem to be more inclined to protect systems in presence of uncertainty about security events evaluations.

As future work, we will extend the analysis by allowing for additional metrics to be considered, such as cost of attack, allowing us to study another financial index, namely return on attack (ROA). With both ROA and ROI, we quantify the nature of the competition between the attacker and the defender. We will study how uncertainty might affect such a competition, and how the best countermeasures can be selected under uncertainty about the two indexes.

References

1. Al-Hadharami, N., Collinson, M., Oren, N.: Modelling security risk scenarios using subjective attack trees. In: Proceedings of the 15th International Conference on Risks and Security of Internet and Systems (CRISIS 2020). p. To appear. Springer (2020)
2. Bistarelli, S., Dall'Aglio, M., Peretti, P.: Strategic games on defense trees. In: International Workshop on Formal Aspects in Security and Trust. pp. 1–15. Springer (2006)
3. Bistarelli, S., Fioravanti, F., Peretti, P.: Defense trees for economic evaluation of security investments. In: First International Conference on Availability, Reliability and Security (ARES'06). pp. 8–pp. IEEE (2006)
4. Cerutti, F., Kaplan, L., Kimmig, A., Şensoy, M.: Probabilistic logic programming with beta-distributed random variables. In: Proc. AAAI. pp. 7769–7776 (2019)
5. Daly, L.: Simple sas macros for the calculation of exact binomial and poisson confidence limits. Computers in biology and medicine **22**(5), 351–361 (1992)
6. Edge, K., Raines, R., Grimaila, M., Baldwin, R., Bennington, R., Reuter, C.: The use of attack and protection trees to analyze security for an online banking system. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07). pp. 144b–144b. IEEE (2007)
7. Edge, K.S.: A framework for analyzing and mitigating the vulnerabilities of complex systems via attack and protection trees. Tech. rep., AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF ENGINEERING AND . . . (2007)
8. Edge, K.S., Dalton, G.C., Raines, R.A., Mills, R.F.: Using attack and protection trees to analyze threats and defenses to homeland security. In: MILCOM 2006-2006 IEEE Military Communications conference. pp. 1–7. IEEE (2006)
9. Jøsang, A.: Subjective logic. Springer (2016)
10. Julious, S.A.: Two-sided confidence intervals for the single proportion: comparison of seven methods by robert g. newcombe, statistics in medicine 1998; 17: 857–872. Statistics in medicine **24**(21), 3383–3384 (2005)
11. Julious, S.A.: Calculation of confidence intervals for a finite population size. Pharmaceutical Statistics **18**(1), 115–122 (2019)
12. Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P.: Foundations of attack–defense trees. In: International Workshop on Formal Aspects in Security and Trust. pp. 80–95. Springer (2010)
13. Lallemant, D., Kiremidjian, A.: A beta distribution model for characterizing earthquake damage state distribution. Earthquake Spectra **31**(3), 1337–1352 (2015)
14. Pieters, W., Davarynejad, M.: Calculating adversarial risk from attack trees: Control strength and probabilistic attackers. In: Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, pp. 201–215. Springer (2014)
15. Roy, A., Kim, D.S., Trivedi, K.S.: Cyber security analysis using attack countermeasure trees. In: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research. pp. 1–4 (2010)
16. Roy, A., Kim, D.S., Trivedi, K.S.: Attack countermeasure trees (act): towards unifying the constructs of attack and defense trees. Security and Communication Networks **5**(8), 929–943 (2012)
17. Sonnenreich, W., Albanese, J., Stout, B., et al.: Return on security investment (rosi)-a practical quantitative model. Journal of Research and practice in Information Technology **38**(1), 45 (2006)