


# Subjective Attack Trees: Security Risk Modeling Under Second-Order Uncertainty

Nasser Al-Hadhrani, University of Technology and Applied Sciences, Oman\*

 <https://orcid.org/0000-0003-2484-7444>

## ABSTRACT

Subjective attack trees (SATs) extend traditional attack trees by taking into account the uncertainty about the probability values of security events. Assigning precise values is often difficult due to lack of knowledge, or insufficient historical data, making the evaluation of risk in existing approaches unreliable, and therefore unreliable security decisions. With SATs, the author seeks to better reflect the reality underpinning the model and offer a better approach to decision-making via the modeling of uncertainty about the probability distributions in the form of subjective opinions, resulting in a model taking second-order uncertainty into account. The author further discusses how to conduct security analysis, such as risk measuring and security investments analysis, under the proposed model. Security investments analysis requires first to incorporate the model with countermeasures and then study how these countermeasures reduce risk in the presence of uncertainty about probability values. The importance and advantage of the SAT model are demonstrated through extended examples.

## KEYWORDS

Attack Trees, Beta Distributions, Decision Analysis, Risk Analysis, Subjective Logic

## INTRODUCTION

An *attack tree* (AT; Schneier, 1999) is a security paradigm used to define and model all possible attack scenarios against a system in a structured, hierarchical way. The general idea is to analyse how a system can be attacked, and this is done by identifying one or more attack goals against a system and then breaking down each goal into sub-goals (or sub-attacks). A simple example AT is shown in Figure 1, which depicts the possible scenario of infecting a computer by putting a virus on the system and executing the virus. Putting a virus on the system is done by either sending an email containing a malicious attachment *or* distributing a USB stick. The leaves of the tree represent the actions (also referred to as *security events*) an attacker can perform in order to complete the attack.

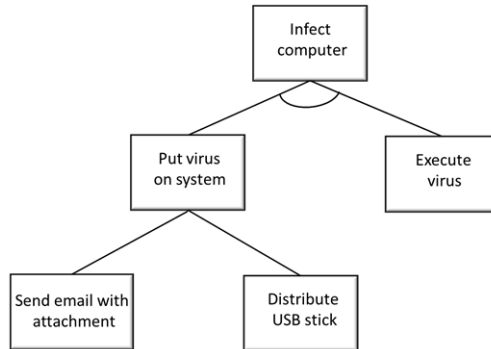
In ATs, reasoning about an attack is done by first evaluating the likelihood of the leaves (i.e., security events), and then propagating the likelihood values to the top of the tree to compute the likelihood of the root node. In ATs, therefore, the main goal of security analysis is to answer the question: What is the likelihood that an attacker can successfully achieve their goal (i.e., the top event

DOI: 10.4018/IJBASC.320498

\*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

Figure 1. An example attack tree model. Here, the infect computer node represents an AND node, while the put virus on system node is an OR node



node in the tree, e.g., infect a computer as in Figure 1)? Traditionally, such an evaluation is done by assigning probability values to the security events. However, assigning precise values is often difficult in the domain of cybersecurity due to lack of knowledge or insufficient historical data, making the answer to the above question, and therefore the outcomes of risk analysis, unreliable.

Unreliability of likelihood values could lead to unreliable outcomes for risk and security analysis in general because, in order to conduct such analysis, it is essential first to know the likelihood of attacks. Therefore, to have a sound and reliable risk analysis of attack trees, the likelihood of security events should be correctly evaluated, and, in case there is uncertainty around the evaluation, we argue that such uncertainties must be explicitly expressed and reasoned with during the analysis. Doing so would better inform the decision-makers about uncertainties affecting the assessment of risk scenarios and enable them to use finer-grained tools to make a decision based on, for instance, their risk attitudes.

In 2021, my colleagues and I proposed a novel attack tree model, called a *subjective attack tree* (SAT), to take into account the uncertainty about the probabilities of security events, via subjective opinions (Al-Hadhrani et al., 2021). In *subjective logic* (Jøsang, 2016), a subjective opinion represents the probability distribution of a random variable complemented by an *uncertainty* degree about the distribution. The modelling of uncertainty about probability distributions in the form of subjective opinions would produce a model that takes *second-order uncertainty* (i.e., uncertainty about probabilities) into account.

In 2020, my colleagues and I extended the model of SAT to consider performing a complete security analysis, such as risk measuring and security investments analysis (using the index of *return on investment*—ROI; Al-Hadhrani et al., 2020). Compared to the security analysis in traditional ATs, such analysis in SATs is carried out in the presence of uncertainty over the probabilities of security events.

In this paper, the author extends on these developments and attempts to address some of their limitations through (a) providing a general form of propagation rules of subjective opinions in SATs to deal with the propagation of any number of input security events, (b) discussing the incorporation of countermeasures into the SAT model when the effectiveness values of these countermeasures are given as precise values in the range of  $[0, 1]$  and when given as uncertain values (e.g., due to uncertainties regarding their effectiveness), and (c) extending the discussion of risk analysis in (Al-Hadhrani et al., 2020) to discuss risk measuring based on second order moment matching which approximates risk as a beta distribution.

The rest of the paper is organised as follows. The following section provides an overview of attack trees and subjective logic. Next, the SAT model is presented, and the propagation method of subjective opinions in the model is demonstrated. Following this, the security analysis in the SAT

model is discussed. The discussion includes conducting risk computation, adding countermeasures to the model, and performing security investments analysis using the index of ROI to select the most profitable security controls for implementation. An illustrative security analysis example using the SAT model is given in the subsequent section. After that, the importance and advantages of the proposed model are demonstrated through a comparison model with the classic probabilistic attack tree model. The discussion section evaluates the proposed model, and finally, some promising future directions for this research are provided.

## BACKGROUND

### Attack Trees and Related Work

Attack trees (ATs) were first introduced in 1999 by Schneier as tools to analyse and evaluate all possible attack scenarios against complex systems in a structured, hierarchical way (Schneier, 1999). Recently, a number of computer-based models and systems are developed such that the security aspect in these systems is being evaluated using the AT model (for example, see Krichen et al., 2019; Scala et al., 2022; Valluripally et al., 2020; Shang et al., 2019). The general idea of ATs is to identify one or more *attack goals* against a system and then break down each goal into sub-goals (or sub-attacks), which can be further decomposed into other sub-goals until reaching a state where sub-attacks cannot be further refined. These final sub-attacks, representing the leaves of an AT, are the basic security events (or actions) an attacker can perform—by exploiting existing vulnerabilities—to achieve their overall goal, i.e., the root node of an AT. A node's children can be decomposed in a conjunctive or disjunctive manner. The former requires that all of the node's children be satisfied in order to complete an attack, while with the latter, at least one of the child nodes has to be satisfied.

The values of nodes in a tree can take on different forms, depending on the security attributes or properties that need to be analysed. Such values may represent the probability of success of a given attack, the likelihood that an attacker will try a given attack, the impact of an attack, and so on. Among these various input parameters used in ATs, the *likelihood of attack* parameter represents one of the core input parameters required to conduct security analysis, as it allows one to determine how likely a system can be attacked. Having determined the likelihood, it is possible after that to extend the security analysis to involve, for example, risk measuring, or conducting security investments analysis to select implementable countermeasures. However, security events often occur in a context of uncertainty, and security analysts should analyse the potential uncertainties around them for efficient identification, management, and evaluation of risk (Couce-Vieira et al., 2017).

The most common approach to evaluate likelihoods in the literature is the use of the probabilistic approach (e.g., Buldas et al., 2020; K. Edge et al., 2007; Kumar & Stoelinga, 2017; Pieters & Davarynejad, 2014; Roy et al., 2010; P. Wang et al., 2012), which provides precise values, as probability distributions, for likelihoods. In this approach, however, eliciting accurate probabilities is usually difficult due to a lack of expertise or insufficient historical data, meaning that the results obtained from using such an approach could be unreliable, and therefore unreliable security decisions (Kaplan & Ivanovska, 2018). Furthermore, using the probabilistic approach, we cannot model situations of ignorance, expressed by “I don't know” (Jøsang, 2016), or situations of high uncertainties as a result of poor knowledge for assigning probabilities.

Other approaches proposed to model uncertainty about likelihoods in risk analysis models, aiming to address the limitations of the probabilistic approach, is the use of interval analysis (Jürgenson & Willemson, 2007) and fuzzy numbers (Buoni et al., 2010; Zhang et al., 2017). In the interval analysis approach, a range of possible values, bounded by lower and upper values, is defined (rather than just a single value) to express possible probabilities for likelihoods. Similarly, with the fuzzy numbers approach, a range of possible values is also defined, but additionally, the approach determines the most likely value within the range, having assigned a possibility of one to this value, while others are assigned lower possibilities (i.e., membership degrees). In these approaches, however, specifying

lower and upper bounds (or determining the most likely value in the fuzzy numbers approach) does not resolve the issue of how these values were precisely determined, that is, in case of insufficient historical data, for example, how can one be certain that the probability is bounded by two known values and therefore cannot be less than the lower value nor greater than the upper value?

## Subjective Logic

*Subjective logic* (Jøsang, 2016) is a formalism for reasoning under uncertainty that extends the probabilistic logic to allow for second-order uncertainty to be expressed about probability values, via so-called *subjective opinions*. In subjective logic, a subjective opinion represents the probability distribution of a random variable complemented by an *uncertainty* degree about the distribution. Consider 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  $p_{\underline{x}}$  (i.e.,  $1 - p_x$ ) that  $X$  is *false*. This makes  $X$  a binary random variable over the domain  $X = \{x, \underline{x}\}$ . If little evidence supporting this proposition is available, or if there is a lack of relevant knowledge regarding the truth of the statement, then we will be unable to obtain the exact probabilities  $p_x$  and  $p_{\underline{x}}$ . A subjective opinion, expressed in terms of both the belief itself and the uncertainty in this belief, models such a situation better. In the security domain, such subjective opinions are clearly useful. In subjective logic, two types of subjective opinions are defined: *binomial* opinions (opinions over binary frames, i.e., frames with only two possible states) and *multinomial* opinions (opinions on a frame larger than binary). This paper deals with only binomial opinions.

### Definition 1: Binomial Opinion

Let  $X = \{x, \underline{x}\}$  be a state space containing  $x$  and its complement  $\underline{x}$ . A binomial opinion about the truth of state  $x$  is the tuple  $\omega_x = \langle b_x, d_x, u_x, a_x \rangle$ , where  $b_x$  is the belief mass in support of  $x$  being true,  $d_x$  is the belief mass in support of  $x$  being false,  $u_x$  is the amount of uncommitted belief mass (i. e., uncertainty), and  $a_x$  is the prior probability, also called the *base rate*, in the absence of committed belief mass. Further, these components must satisfy the conditions that  $b_x + d_x + u_x = 1$  and  $b_x, d_x, u_x, a_x \in [0, 1]$ .

For a given binomial opinion  $\omega_x$ , the corresponding *projected probability distribution*  $P(x) : x \rightarrow [0, 1]$  is determined by

$$P(x) = b_x + a_x \cdot u_x \quad (1)$$

where  $P(x)$  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  $u_x = 0$ .

## Subjective Logic Operators

Subjective logic provides a set of operators where input and output arguments take the form of opinions. There is a standard set of logical operators (such as conjunction, disjunction, and negation) used in domains containing uncertainty, and, more specifically, domains in which there are opinions regarding the truth or falsehood of a (set of) domain elements. Here, only three operators are needed, namely the *conjunction* (also called *multiplication*), *disjunction* (also called *co-multiplication*), and *complement* (also called *negation*) operators.

**Definition 2: Conjunction Operator**

Given two opinions,  $\omega_x = \langle b_x, d_x, u_x, a_x \rangle$  and  $\omega_y = \langle b_y, d_y, u_y, a_y \rangle$ , where  $x$  and  $y$  belong to independent frames of discernment, we compute the conjunction of the two opinions,  $\omega_{x \wedge y}$ , as

$$\begin{aligned} b_{x \wedge y} &= b_x b_y + \frac{(1 - a_x) a_y b_x u_y + a_x (1 - a_y) u_x b_y}{1 - a_x a_y}, \\ d_{x \wedge y} &= d_x + d_y - d_x d_y, \\ u_{x \wedge y} &= u_x u_y + \frac{(1 - a_y) b_x u_y + (1 - a_x) u_x b_y}{1 - a_x a_y}, \text{ and} \\ a_{x \wedge y} &= a_x a_y. \end{aligned}$$

By using the symbol  $(\cdot)$  to denote this operator, multiplication of opinions can be written as  $\omega_{x \wedge y} = \omega_x \cdot \omega_y$ .

**Definition 3: Disjunction Operator**

Given two opinions,  $\omega_x = \langle b_x, d_x, u_x, a_x \rangle$  and  $\omega_y = \langle b_y, d_y, u_y, a_y \rangle$ , where  $x$  and  $y$  belong to independent frames of discernment, we compute the disjunction of the two opinions,  $\omega_{x \vee y}$ , as

$$\begin{aligned} b_{x \vee y} &= b_x + b_y - b_x b_y, \\ d_{x \vee y} &= d_x d_y + \frac{a_x (1 - a_y) d_x u_y + (1 - a_x) a_y u_x d_y}{a_x + a_y - a_x a_y}, \\ u_{x \vee y} &= u_x u_y + \frac{a_y d_x u_y + a_x u_x d_y}{a_x + a_y - a_x a_y}, \text{ and} \\ a_{x \vee y} &= a_x + a_y - a_x a_y. \end{aligned}$$

By using the symbol  $(\sqcup)$  to denote this operator, co-multiplication of opinions can be written as  $\omega_{x \vee y} = \omega_x \sqcup \omega_y$ .

**Definition 4: Complement Operator**

Given an opinion  $\omega_x = \langle b_x, d_x, u_x, a_x \rangle$  where  $x$  belongs to a frame of discernment, we may compute the complement opinion  $\omega_{\neg x}$ , known as the propositional negation, as

$$\begin{aligned} b_{\neg x} &= d_x, \\ d_{\neg x} &= b_x, \\ u_{\neg x} &= u_x, \\ a_{\neg x} &= 1 - a_x. \end{aligned}$$

## Binomial Opinions and Beta Distributions

A binomial opinion translates directly into a beta distribution. To understand such a connection between binomial opinions and beta distributions, this section begins with an overview of beta distributions and then discusses how subjective opinions are translated into beta distributions and vice versa. When probabilities are uncertain (e.g., due to limited observations), such an uncertainty can be captured by a beta distribution (Gupta & Nadarajah, 2004), i.e., a distribution of possible probabilities. Let us consider a binary variable  $X$  that can take on the value of true or false (i.e.,  $X = x$  or  $X = \underline{x}$ ). As discussed earlier, there is an underlying ground truth probability  $p_x$  that  $X$  is *true*, and  $p_{\underline{x}}$  (i.e.,  $1 - p_x$ ) that  $X$  is *false*. If  $p_x$  is drawn from a beta distribution, it has the following *probability density function* (PDF; Cerutti et al., 2019):

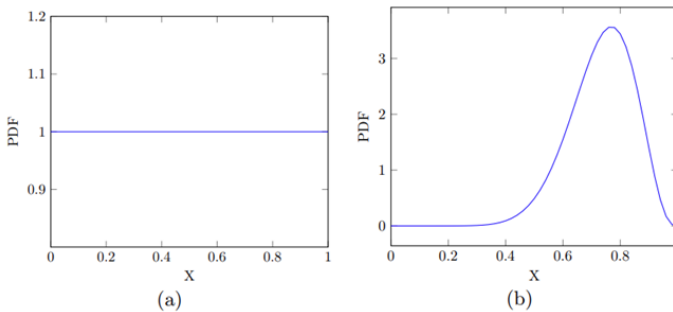
$$f_{\beta}(p_x; \alpha) = \frac{1}{\beta(\alpha_x, \alpha_{\underline{x}})} p_x^{\alpha_x - 1} (1 - p_x)^{\alpha_{\underline{x}} - 1}$$

for  $0 \leq p_x \leq 1$ , where  $\beta(\cdot)$  is the beta function and the beta parameters  $\alpha_X = \langle \alpha_x, \alpha_{\underline{x}} \rangle$ , such that  $\alpha_x > 1$ ,  $\alpha_{\underline{x}} > 1$ .

The value of  $X$  can be determined from  $N_{ins}$  independent observations. Let  $n_x$  be the total number of observations supporting  $X = x$ , and  $n_{\underline{x}}$  be the total number of observations supporting  $X = \underline{x}$ , then the beta parameters  $\alpha_X = \langle n_x + W a_x, n_{\underline{x}} + W(1 - a_x) \rangle$ , where  $a_x$  is the prior assumption, and  $W$  is a prior weight indicating the strength of the prior assumption. In this paper, unless specified otherwise, we assume  $\forall X, a_x = 0.5$ , and  $W = 2$ , to obtain the prior beta distribution as a uniform distribution, which is an uninformative prior. By making  $W = 2$  and  $a_x = 0.5$ , the above formula of beta parameters thus becomes  $\alpha_X = \langle n_x + 1, n_{\underline{x}} + 1 \rangle$ , which reflects the parameters of a posterior beta distribution when having a likelihood in a Bernoulli distribution and a uniform prior expressed as a beta distribution with parameters  $\langle 1, 1 \rangle$ . Suppose, for example, that the total observations for  $X$  is 10, 7 of which support  $X = x$  (and thus 3 observations support  $X = \underline{x}$ ), the beta parameters then becomes  $\langle 11, 4 \rangle$ . Figure 2 shows the beta distribution of this example.

Given a beta-distributed random variable  $X$ , its Dirichlet strength  $S_X$  and mean  $\mu_X$  are computed using the following two equations, respectively:

**Figure 2. Example beta distributions: (a) a prior beta distribution with parameters  $\langle 1, 1 \rangle$ , and (b) a posterior beta distribution with parameters  $\langle 11, 4 \rangle$**



$$S_X = \alpha_x + \alpha_{\underline{x}} \quad (2)$$

$$\mu_X = \frac{\alpha_x}{S_X} \quad (3)$$

From these two equations, the beta parameters can be equivalently written as:

$$\alpha_X = \langle \mu_X S_X, (1 - \mu_X) S_X \rangle \quad (4)$$

The variance of a beta-distributed random variable  $X$  is:

$$\sigma_X^2 = \frac{\mu_X (1 - \mu_X)}{S_X + 1} \quad (5)$$

and from this equation we can rewrite  $S_X$  as:

$$S_X = \frac{\mu_X (1 - \mu_X)}{\sigma_X^2} - 1 \quad (6)$$

As mentioned earlier, there is a correspondence between beta distributions and binomial opinions. The mapping from a beta-distributed random variable  $X$  with parameters  $\alpha_X = \langle \alpha_x, \alpha_{\underline{x}} \rangle$  to a subjective opinion is defined by:

$$\omega_X = \left\langle \frac{\alpha_x - W a_x}{S_X}, \frac{\alpha_{\underline{x}} - W (1 - a_x)}{S_X}, \frac{W}{S_X}, a_x \right\rangle \quad (7)$$

With this transformation, the mean of  $X$  is equivalent to the projected probability  $P(X)$  defined in Equation 1, and the Dirichlet strength is inversely proportional to the uncertainty of an opinion, which can be directly computed from the subjective opinion as:

$$S_X = \frac{W}{u_x} \quad (8)$$

Conversely, a subjective opinion  $\omega_X$  translates directly into a beta distributed random variable. Given a subjective opinion  $\omega_X = \langle b_x, d_x, u_x, a_x \rangle$ , the corresponding beta parameters  $\alpha_X = \langle \alpha_x, \alpha_{\underline{x}} \rangle$  are determined by:

$$\alpha_X = \left\langle \frac{W}{u_x} b_x + W a_x, \frac{W}{u_x} d_x + W(1 - a_x) \right\rangle \quad (9)$$

Cerutti et al. (2019) defined some operators that can be applied on independent beta distributed random variables such as *sum* and *product*, designed as alternatives to the operators of addition and multiplication on subjective opinions, and thus are useful when converting opinions into corresponding beta distributions. These operators approximate the resulting distribution as a beta distribution via moment matching on mean and variance. In this paper, we make use of the product operator.

#### Definition 5: Product

Given  $X$  and  $Y$  as two beta-distributed random variables, the product of  $X$  and  $Y$  is defined as the beta-distributed random variable  $Z$  such that  $\mu_Z = \mu_{XZ} = \mu_X \mu_Y$  and  $\sigma_Z^2 = \sigma_{XY}^2 = \sigma_X^2(\mu_Y)^2 + \sigma_Y^2(\mu_X)^2 + \sigma_X^2 \sigma_Y^2$ . By knowing the mean ( $\mu_Z$ ) and variance ( $\sigma_Z^2$ ) of a beta-distributed random variable  $Z$ , it is possible to compute the beta parameters by first determining the Dirichlet strength according to Equation 6, and then obtaining the beta parameters using Equation 4.

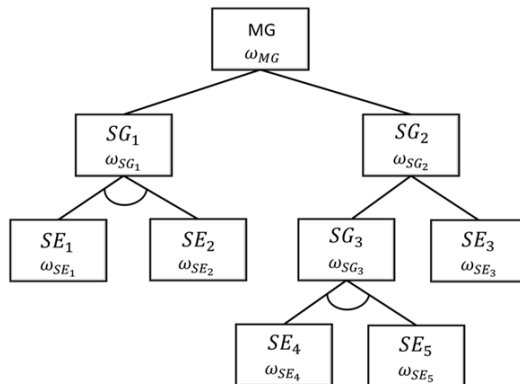
## SUBJECTIVE ATTACK TREES

### The Model

Subjective attack trees (SATs) extend the classical probabilistic attack trees by allowing for uncertainty degrees about the probabilities of security events to be explicitly expressed via subjective opinions, resulting in a model taking second-order uncertainty into account. Therefore, the tree structure in SATs is not different from the one in traditional ATs in that it also allows for the (conjunctive or disjunctive) decomposition of the main goal of an attacker into sub-goals, except that the input parameters represent subjective opinions rather than probabilities.

Figure 3 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  $\omega_{SE_1}$  and  $\omega_{SE_2}$ .

Figure 3. A subjective attack tree (SAT) model uses subjective opinions as input parameters to capture uncertainty degrees about the events' likelihoods. Here,  $\omega_i$  is a subjective opinion capturing aspects of the likelihood of event  $i$





The subjective opinion on sub-goal 1 ( $\omega_{SG_1}$ ) is computed from the *conjunction* of  $\omega_{SE_1}$  and  $\omega_{SE_2}$ , and the subjective opinion on the main goal ( $\omega_{MG}$ ) is computed from the *disjunction* of  $\omega_{SG_1}$  and  $\omega_{SG_2}$ . The subjective opinion on MG represents the *belief* and *disbelief* that an attacker can successfully achieve their main goal, complemented by an *uncertainty* degree about such belief and disbelief masses.

### Propagation of Subjective Opinions in SATs

Subjective opinions in the SAT model are assigned to the leaves, and then propagated up the tree to compute a subjective opinion about the root node. Such propagation is achieved by solving two types of gates between nodes, namely the AND gate and OR gate.

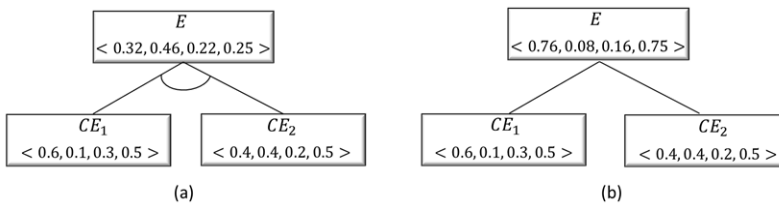
#### Propagation Through an AND Gate

An AND gate signifies that the output event  $E$  occurs if all the input events have accrued simultaneously. To compute an output from AND gate, the conjunction operator of subjective logic is used. Let  $E$  be an event node in a SAT, where  $E \in \{MG, SG_i\}$ . In other words,  $E$  is the main goal  $MG$  (i.e., the root node), or any sub goal ( $SG_i$ ) in a SAT. Let  $\omega_{CE_1}, \omega_{CE_2}, \dots, \omega_{CE_n}$  be the subjective opinions on the children nodes of the event  $E$ , which *all* must be satisfied to ensure the occurrence of  $E$ . We compute a subjective opinion on  $E$  using the following AND gate's propagation rule  $\omega_E = \omega_{CE_1} \cdot \omega_{CE_2} \cdot \dots \cdot \omega_{CE_n}$ , where  $\cdot$  is the conjunction operator, and  $\omega_{CE_i} = \omega_{SE_i}$  for any  $i \in \{1, 2, \dots, n\}$  in case that  $E$  is the direct parent of the security events (i.e., the leaves), or  $\omega_{CE_i}$  is computed first from its children nodes using either the same propagation rule or the OR-gate's propagation rule we discuss below. Figure 4a shows an example computation of a subjective opinion on event  $E$  via AND gate.

#### Propagation Through an OR Gate

An OR gate signifies that the output event  $E$  occurs if at least one of the input events has accrued. To compute an output from OR gate, the disjunction operator of subjective logic is used. Let  $E$  be an event node in a SAT, where  $E \in \{MG, SG_i\}$ . In other words,  $E$  is the main goal  $MG$  (i.e., the root node), or any sub goal ( $SG_i$ ) in a SAT. Let  $\omega_{CE_1}, \omega_{CE_2}, \dots, \omega_{CE_n}$  be the subjective opinions on the children nodes of the event  $E$ , which *at least one* of them must be satisfied to ensure the occurrence of  $E$ . We compute a subjective opinion on  $E$  using the following OR gate's propagation rule  $\omega_E = \omega_{CE_1} \sqcup \omega_{CE_2} \sqcup \dots \sqcup \omega_{CE_n}$ , where  $\sqcup$  is the disjunction operator, and  $\omega_{CE_i} = \omega_{SE_i}$  for any  $i \in \{1, 2, \dots, n\}$  in case that  $E$  is the direct parent of the security events (i.e., the leaves), or  $\omega_{CE_i}$  is computed first from its children nodes using either the same propagation rule or the AND gate's

Figure 4. Computing a subjective opinion on event E through (a) AND gate, and (b) OR gate



propagation rule we discussed above. Figure 4b shows an example computation of a subjective opinion on event  $E$  via OR gate.

## SECURITY ANALYSIS IN SATS

In this section, we discuss how to conduct security analysis (e.g., risk computation and security investments analysis) under the proposed SAT model. This requires us to enrich the model with additional metrics and components such as impact (for risk computation) and countermeasures (and their costs) for security investments analysis to determine which countermeasures are profitable, using the index of ROI (Sonnenreich et al., 2006). Since likelihoods in the SAT model are subjective opinions (i.e., there is uncertainty about the probabilities), the security analysis differs from the analysis of security in traditional ATs models. Therefore, it is essential to study how risk or security investments analysis is conducted, simultaneously showing how to handle uncertainties in the model for effective decision analysis.

### Risk Computation

In the context of ATs, the *risk* to a system refers to the system's risk with respect to a particular attack scenario, i.e., risk at the root node. Here, two measures need to be taken into consideration, the first is the probability of attack success, and the other one is the amount of damage that an attack scenario can render to the system. Combining the two, risk to the system can be defined as the expected value of the impact (review the discussion in Roy et al., 2012):

$$\text{Risk} = \text{probability} \times \text{impact} \quad (10)$$

The likelihood of attack success in our SAT model is a subjective opinion, and so the risk cannot be simply computed using Equation 10 directly—we cannot directly multiply a subjective opinion (which represents the likelihood) by a number (representing the impact). Also, sometimes the impact can be represented as a beta distribution (rather than a single value) to express confidence in the level of impact, such as the approach given by Lallemand and Kiremidjian (2015) for characterizing earthquake damage. Here, representing the impact as a beta distribution in our model would have to be combined with the subjective opinion of the likelihood in order to compute risk (i.e., the expected value of the impact). In this section, we discuss how to calculate risk in the SAT model based on the representation of the impact value (i.e., when the impact is represented as a single value, and when it is given as a beta distribution).

#### *Risk Computation With a Single Value of Impact*

The problem of computing risk in our SAT model using Equation 10 is that the impact value (given it is a single value in the range  $[0, 1]$ ) cannot be directly multiplied by the subjective opinion of the likelihood. One possible way to calculate risk in this case is to multiply the impact value with the *projected probability* of the subjective opinion, meaning that we are considering only the most expected value of risk. However, using this simple approach, we move away from the advantage of keeping the distribution of the likelihood explicit when computing risk in order to enable using finer grained tools to make a decision based on, for example, risk appetite.

Given that the likelihood is a subjective opinion (knowing that subjective opinions translate directly into beta distributions) and the impact is a single value, the risk is a scaled version of the beta distribution with support from zero to the value of impact. It is therefore possible to approximate risk as a regular beta distribution as long as the impact is bounded by one (i.e., within the range  $[0, 1]$ ). To approximate risk as a beta distribution, we perform second order moment matching so that the Dirichlet strength represents the variance. The second order moment matching method has been

discussed further by Kaplan and Ivanovska (2018), but here we briefly discuss the steps to calculate risk in our model based on such a method.

To compute the beta parameters of risk, we need to determine the mean and Dirichlet strength. The mean is calculated by multiplying the impact value with the projected probability of the subjective opinion, i.e.,  $\mu_R = i \times P(x)$ , where  $i$  is the impact value and  $P(x)$  is the projected probability. To compute the Dirichlet strength, we follow the following approach. By using the symbols  $r$ ,  $i$ , and  $p$  to denote risk, impact, and probability, respectively, we write the risk formula (see Equation 10) for simplicity as  $r = i \times p$ . In our approach, impact  $i$  is considered to be deterministic and  $p$  is beta distributed. This makes  $r$  a random variable with expected value:

$$E[r] = i \times E[p] \quad (11)$$

Note that  $E[r] = \mu_R$  (i.e., the mean of risk as discussed above), and so:

$$E[r^2] = i^2 \times E[p^2] \quad (12)$$

where  $E[p^2] = \frac{\alpha_x + 1}{S_x + 1} \cdot E[p]$  (also see Owen, 2008, for the method of moments).

In Equation 12,  $E[p]$  represents the projected probability of the subjective opinion. By knowing  $E[r^2]$ , it is possible to compute the variance of risk as:

$$\sigma_R^2 = E[r^2] - E[r]^2 \quad (13)$$

where  $E[r]^2$  is the square value of  $E[r]$  obtained from Equation 11.

Now having the mean of risk,  $\mu_R$ , and its variance,  $\sigma_R^2$ , we can compute the Dirichlet strength,  $S_R$ , as follows (review Equation 6):

$$S_R = \frac{\mu_R(1 - \mu_R)}{\sigma_R^2} - 1 \quad (14)$$

Finally, knowing the Dirichlet strength  $S_R$  and mean  $\mu_R$ , we compute the beta parameters as  $\alpha_x = \langle \mu_x S_x, (1 - \mu_x) S_x \rangle$ .

### 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  $\mu_R = 0.4 \times 0.7 = 0.28$ , where 0.7 is the projected probability of  $\omega_{SE}$ . Using Equation 12, we obtain  $E[r^2] = 0.4^2 \times 0.51 = 0.0816$ . Now based on Equation 13, we obtain the variance of risk as  $\sigma_R^2 = 0.0816 - 0.28^2 = 0.0031$ . Having the mean of risk as  $\mu_R = 0.28$  and variance as  $\sigma_R^2 = 0.0031$ , we compute the Dirichlet strength using Equation 14 as  $S_R = (0.28 \times (1 - 0.28) / 0.0031 - 1) = 64$ .

Accordingly,  $\alpha = \langle 0.28 \times 64, (1 - 0.28) \times 64 \rangle = \langle 17.9, 46.1 \rangle$ . The beta distribution of risk in this example is shown in Figure 5a.

### Risk Computation With a Beta Distribution Representation of Impact

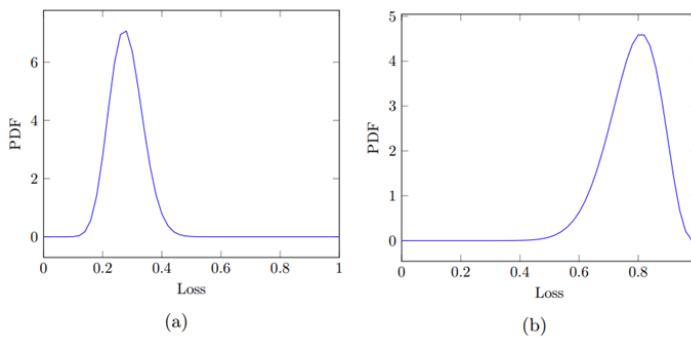
When the impact is given as a beta distribution, risk is measured based on two beta-distributed random variables, representing the impact and likelihood (knowing that subjective opinions for likelihoods can be translated directly into beta distributions). Our approach for calculating risk is therefore based on first translating the subjective opinion into a beta distribution, and then enabling the product of the two beta-distributed random variables according to Definition 5. The following summarises the steps to calculate risk in case that the impact is given as a beta distribution:

1. We translate the given subjective opinion into the corresponding beta distribution (see Equation 9), and then compute its mean and variance via Equation 3 and Equation 5, respectively.
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 Definition 5) to compute the mean and variance of risk.
4. We use these values of mean and variance to calculate the Dirichlet strength of risk using Equation 6.
5. We use the mean and Dirichlet strength of risk to get the beta parameters of risk distribution using Equation 4.

### Example 2

Suppose the subjective opinion about security 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 (loss) distribution is then obtained by first computing the mean and variance of both the likelihood (i.e.,  $\omega_{SE}$ ) and impact distributions. This yields  $\mu_{SE} = 0.95$ ,  $\sigma_{SE}^2 = 0.00226$ ,  $\mu_I = 0.82$ , and  $\sigma_I^2 = 0.0064$ . Using the product operator (see Definition 2.5), we obtain the mean and variance of risk  $R$  as  $\mu_R = 0.78$  and  $\sigma_R^2 = 0.00764$ . The Dirichlet strength is therefore  $S_R = 21.5$ . Based on this, we obtain beta parameters for risk as  $\alpha = \langle 16.8, 4.7 \rangle$ . The risk (loss) distribution is shown in Figure 5b.

Figure 5. The beta distributions of loss (risk) in (a) Example 1 and (b) Example 2, where 0 indicates no risk and 1 indicates that the risk is catastrophic



Since both representations of impact (the single value and beta distribution representation) yield a beta distribution for risk, for simplicity, in the rest of this paper, we model impact through single values. Here, two measures need to be taken into consideration in order to compute risk at the root node: the subjective opinion on the attack success,  $\omega_{goal}$  and the amount of damage (i.e., impact) that an attack scenario can present to the system,  $I_{goal}$ . The propagation of subjective opinions in the attack model to compute  $\omega_{goal}$  is discussed in the previous section, and the propagation of impact values to compute  $I_{goal}$  is discussed in (K. S. Edge et al., 2006). However, since our impact scale is  $[0, 1]$  and not  $[1, 10]$ , we redefine the propagation rule of impact values defined in (K. S. Edge et al., 2006) as follows (see Table 1, which summarises the formulae for computing the impact in our model):

$$1 - \prod_{i=1}^n (1 - I_{A_i})$$

where  $n$  is the number of children nodes and each  $A_i$  is the unique name of a child node. Figure 6 shows an example propagation of impact values, as well as subjective opinions, to compute risk at the root node. 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.

### 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 translate directly into beta distributions) rather than single values. For decision analysis, it is important therefore to handle the uncertainty in such metrics, as we will see in the next section when coming to analyse security investments. We discuss in this section two possible approaches to reason about risk (or about likelihood) in the presence of uncertainty about the values. These approaches are: (a) reasoning with the most expected value, and (b) 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 of risk (or likelihood) to reason about risk under the most expected scenario. For likelihoods, the most expected value is the projected probability of the subjective opinion, and it is the distribution's mean when reasoning about risk. For example, in Example 2 discussed earlier, one could make a decision based on the most expected scenario of risk using the value of 0.78, which represents the mean of risk as shown in Figure 5b.

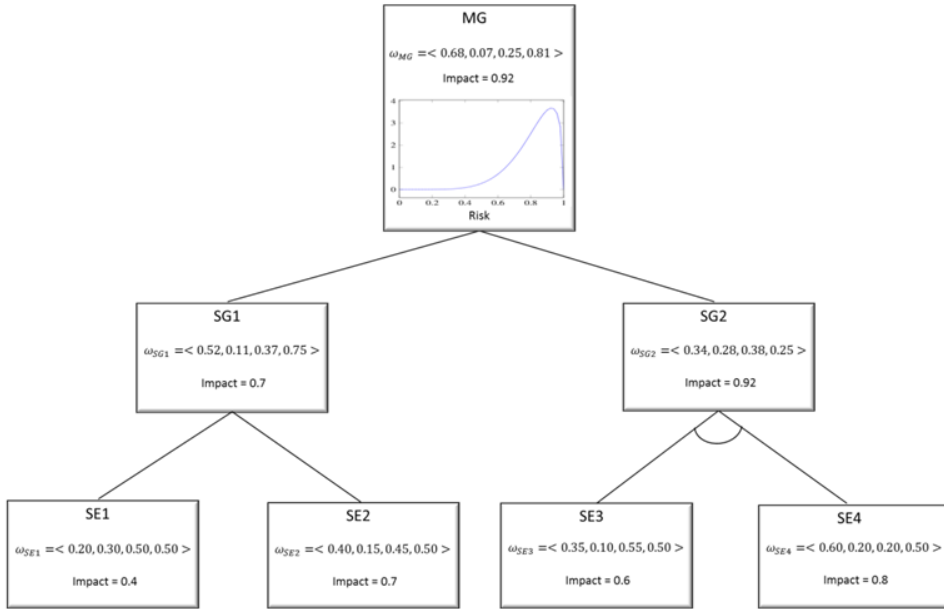
#### Approach 2: Reasoning With Confidence Intervals for Best- and Worst-Case Scenarios

Unlike in the previous approach, which represents risk as a single value, risk in this approach is represented by a range of possible values, determined by lower and upper bounds with a given

Table 1. Formulae for attack impact computation

Gate type	Attack impact
AND gate	$1 - \prod_{i=1}^n (1 - I_{A_i})$
OR gate	$\max_{i=1}^n I_{A_i}$

Figure 6. An example SAT showing propagation of impacts and subjective opinions. The top event shows the system risk with a beta distribution representation, calculated from the subjective opinion  $\langle 0.68, 0.07, 0.25, 0.81 \rangle$  and impact value of 0.92



confidence level, therefore allowing one to consider additional scenarios for risk such as the best and worst-case scenarios. The approach thus offers the advantage of conducting a what-if analysis, for example, by analysing the outcome according to different possible values.

In the literature, several approaches exist to compute confidence intervals of a beta distribution (e.g., Newcombe, 1998; Daly, 1992; Julious, 2005). A simple approach is the one Julious discussed (2019), 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  $\alpha$  is the level of statistical significance,  $k$  the number of events observed, and  $n$  the sample size.  $BETAINV()$  is the cumulative distribution function (taken from Excel) of a beta distribution. The lower and upper bounds calculated from the two equations above will determine the range of possible values that the risk value is likely to be within.

As an example, consider again the example of Figure 5b, which represents the beta distribution of risk with shape parameters  $\alpha = \langle 16.8, 4.7 \rangle$ . The sample size  $n$  represents  $\alpha_x + \alpha_{\bar{x}} = 21.5$ . The number of events observed  $k$ , as discussed in Section 2.6.2, represents  $n_x$  in the formula  $\alpha_x = \langle n_x + W a_x, n_{\bar{x}} + W(1 - a_x) \rangle$ . If we assume (as discussed earlier) that  $W = 2$  and  $a_x = 0.5$ , then  $k$  in this example is 15.8. For a 95% confidence interval, the statistical significance level  $\alpha$  takes the value 0.05. Using the  $BETAINV$  function in Excel, we obtain the lower bound as 0.50 and

the upper bound as 0.89. Therefore, the 95% confidence interval in this example is [0.50, 0.89]. This means that we are 95% confident that the risk value is likely to be within this interval, and so, additional risk scenarios could be considered as part of dealing with uncertainty.

## Analyzing Security Investments

In this section, we discuss security investment analysis in SATs. In order to conduct such an analysis, we first need to incorporate the model with countermeasures and study how these countermeasures reduce risk in the presence of subjective opinions. Following this, we conduct an investment analysis using the index of ROI for countermeasures.

### Adding Countermeasures to SATs

The SAT model presented in the third section does not take into account defence mechanisms which can be implemented by the defending organization or the costs sustained for security investments. In this section, we discuss the addition of countermeasures to the SAT model, studying how these countermeasures reduce risk (here, likelihoods) in the presence of uncertainty about probability values (i.e., in the presence of subjective opinions). Each added countermeasure should be associated with a value representing the effectiveness of the countermeasures in reducing risk. In the literature, the effectiveness value of a countermeasure is expressed as a percentage or as a value in the interval  $[0, 1]$  (see for example (Roy et al., 2012; Bistarelli et al., 2006)), and the estimation of such a value is typically determined by expert knowledge. The likelihood of an attack in the presence of a countermeasure is then calculated by multiplying the attack probability without the countermeasure by the countermeasure's effectiveness value subtracted from one. However, when there is uncertainty about the likelihood (as in SATs), the calculation should be different.

Our approach to calculating the likelihood (i.e., the subjective opinion) on a node when adding a countermeasure (with an effectiveness greater than 0) to it is based on ensuring that the projected probability of the resulting subjective opinion from the application of the countermeasure is obtained as if the projected probability of the original subjective opinion (i.e., the subjective opinion without a countermeasure) was reduced in the same way a probability value is reduced as a result of the application of a countermeasure. In other words, a countermeasure reduces (indirectly) the projected probability of the subjective opinion in the same way it does with probability values. For example, if the projected probability on a node is 0.8, then adding a countermeasure of 0.5 effectiveness would reduce the projected probability to 0.4 (based on the calculation discussed above). To achieve this, we assume here that the effectiveness value would affect only the belief mass and base rate of the subjective opinion while maintaining the same uncertainty value. The disbelief mass is then calculated by subtracting the total value of the resulting new belief mass and uncertainty from one. This process ensures to have a subjective opinion that has a reduced projected probability according to the effectiveness value of the countermeasure. Formally, assuming  $\omega_{SE} = \langle b_{se}, d_{se}, u_{se}, a_{se} \rangle$  is the subjective opinion about a security event  $SE$ ,  $CM$  is a potential countermeasure to reduce risk, and  $E_{CE}$  is the countermeasure effectiveness, we compute the opinion about  $SE$  with countermeasure  $CM$ , denoted by  $\omega'_{SE} = \langle b'_{se}, d'_{se}, u'_{se}, a'_{se} \rangle$ , as follows:

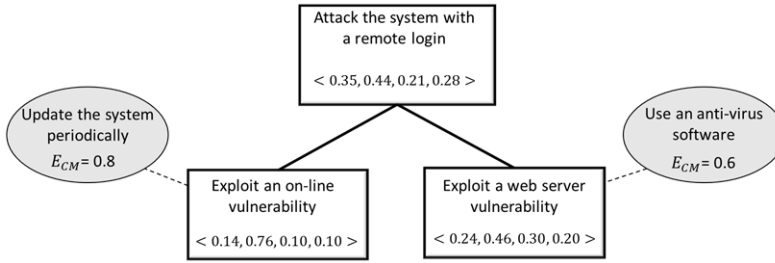
$$b'_{se} = b_{se} \times (1 - E_{CE}),$$

$$a'_{se} = a_{se} \times (1 - E_{CE}),$$

$$u'_{se} = u_{se}, \text{ and}$$

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

Figure 7. A SAT model with two countermeasures (ovals), showing how they reduce likelihoods (i.e., subjective opinions) on the leaves, and subsequently on the root node. The variable  $E_{CM}$  denotes countermeasure effectiveness



Note that in the approach above, we considered, as in existing approaches, the use of precise values in the range  $[0, 1]$  to represent the effectiveness values of countermeasures, ignoring the uncertainty aspect in them as a result of poor knowledge for assigning such values. Since the effectiveness of a countermeasure actually represents the probability of the countermeasure's success (see Roy et al., 2012), therefore, it might be possible, to consider assigning each countermeasure a subjective opinion such that they represent the likelihood (with associated uncertainty degrees) that each countermeasure would be successful in reducing risk. In this case, calculating the likelihood of a node in the presence of a countermeasure is based on multiplying the subjective opinion on the node with the complement of the subjective opinion (review Definition 4) about countermeasure success.

Suppose a countermeasure with an effectiveness value of  $\langle 0.6, 0.2, 0.2, 0.5 \rangle$  is added to a node with likelihood of  $\langle 0.7, 0.1, 0.3, 0.5 \rangle$ . The subjective opinion on the node in the presence of the countermeasure is then calculated as:

$$\langle 0.7, 0.1, 0.3, 0.5 \rangle \cdot \langle 0.2, 0.6, 0.2, 0.5 \rangle = \langle 0.16, 0.64, 0.2, 0.25 \rangle.$$

Since both representations of the effectiveness value (i.e., the single value and subjective opinion representations) yield a subjective opinion on a node, for simplicity, in the rest of this paper, we model countermeasures' effectiveness through single values.

Figure 7 shows two countermeasures (in the ovals) added to the subjective attack tree of attacking a system with a remote login. These countermeasures were added to the nodes of exploiting an online vulnerability (update the system periodically) and exploiting a web server vulnerability (use an anti-virus software) to reduce their likelihoods, which are expressed by the subjective opinions of  $\langle 0.7, 0.2, 0.1, 0.5 \rangle$  and  $\langle 0.6, 0.1, 0.3, 0.5 \rangle$ , respectively. The effectiveness of the two countermeasures are 0.8 and 0.6, respectively. The figure shows the resulting subjective opinions on the nodes after applying these two countermeasures, which led to a change in the risk value on the root node (attack the system with a remote login) from  $\langle 0.88, 0.65, 0.77, 0.75 \rangle$  to  $\langle 0.35, 0.44, 0.21, 0.28 \rangle$ .

### ROI Analysis

We discuss in this section how a security investment is analysed in the SAT model, using the index of ROI, an economic metric that is used to measure the profit obtained by the implementation of a specific countermeasure  $CM_i$ . ROI for a security investment is calculated as (Sonnenreich et al., 2006):

$$ROI = \frac{(\text{Risk exposure} \times \% \text{ Risk mitigated}) - \text{Investment cost}}{\text{Investment cost}}. \quad (15)$$



In AT models, *risk exposure* represents risk at the root node. Depending on the purpose of the model, risk exposure can represent different forms. For example, it can be the likelihood on the root node if the model is concerned only with determining how likely a system can be attacked without considering impact values. Here, the purpose of countermeasures is to reduce the likelihood of attack. Risk exposure could also be the *expected impact* on the root node if impact values are considered in the model, and the countermeasures applied to such models would aim to reduce the overall expected impact.

In this paper, we consider ROI analysis with risk exposure to be defined as the *likelihood* (in our model, the subjective opinion) with regard to the goal (i.e., the top event node). We do so for two reasons: (1) for the sake of simplicity, and (2) because countermeasures do not affect the impact value directly (the impact value at the root node is the same apart from whether there were countermeasures applied or not), but rather affect the likelihood of an event occurrence (see Roy et al., 2012). This means that by reducing likelihoods, the expected impacts are reduced accordingly. We should note here that in case of considering risk exposure to be the expected impact, and since the expected impact in our model is a beta distribution, we can first translate the beta distribution into the corresponding opinion and then follow the same approach discussed below (or alternatively, we consider the beta distribution itself and use the value of mean or any of the confidence interval bounds to represent the value for risk exposure in the formula above, as discussed below).

The *% Risk mitigated* value is the amount of the percentage risk mitigated as a result of applying a specific countermeasure. Unlike with single probabilistic values, it is difficult in our approach to directly calculate such a percentage because the uncertainty value and base rate at the root node might change as a result of applying a countermeasure to the model. Therefore, we must first resolve the uncertainties in the subjective opinions (using one of the approaches discussed in the previous section) in order to be able to compute the percentage risk mitigated, and then use this percentage in the above formula of ROI.

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  $1 - (0.66 / 0.82) = 0.195$ . For abbreviation, we denote such a calculation of risk mitigated by *%RM*.

*Investment cost* is the cost of the applied countermeasure. In this paper, we assume, as in existing approaches, that the cost of a countermeasure is a single value. Based on the discussion above, we re-define ROI for a countermeasure  $CM_i$  as

$$ROI_{CM_i} = \frac{(R_{sys} \times \%RM) - C_{CM_i}}{C_{CM_i}} \quad (16)$$

where  $R_{sys}$  is the system risk, i.e., the subjective opinion on the root node  $\omega_{goal}$ , with an uncertainty treated according to the approaches in the previous section. In other words,  $R_{sys}$  can take on any of the following values: the projected probability of  $\omega_{goal}$ , the lower bound of the desired confidence interval, or its upper bound. *%RM* is computed as demonstrated above;  $1 - (R_{sys-with-CM_i} / R_{sys-without-CM_i})$ .

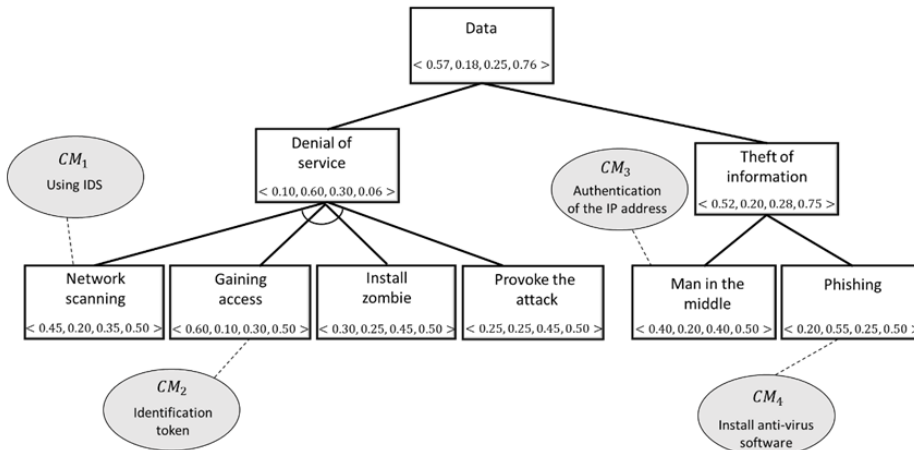
In Equation 16, a countermeasure  $CM_i$  is only profitable if  $(R_{sys} \times \%RM) > C_{CM_i}$  (here,  $C_{CM_i}$  is the cost of the countermeasure  $CM_i$ ), and this is satisfied when the risk value is within the scale of  $[0, 100]$  rather than  $[0, 1]$  (see Bistarelli et al., 2006). Therefore, 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 the value of ROI, the more desirable the investment. Suppose in the example given above, the cost for implementing  $CM_i$  is \$20.  $ROI_{CM_i}$  is then  $(82 \times 0.195) - 20 = -0.2$ . Since ROI is negative, the countermeasure is not profitable.

## ILLUSTRATIVE EXAMPLE

Consider the attack tree example for the data attack scenario presented by Bistarelli et al. (2012); a version of the model with countermeasures is also presented, but for simplicity, we consider here only four countermeasures, as shown in Figure 8. The attack tree model demonstrates two different attack scenarios against data belonging to a hosting service provided by an internet service company. An attacker can consider either (a) damaging the business activity of the company, or (b) accessing data about customers. To damage the business activity of the company, the attacker can perform a denial-of-service attack (DoS) by performing the following attack actions: (a) scanning the network to discover some vulnerabilities, (b) gaining access to a machine, (c) installing a zombie, and (d) performing the attack activating the zombie. The DoS attack node is therefore of the AND type because, in order to successfully perform this attack strategy, the attacker must perform all the actions composing the attack. In order to access data about customers, the attacker can perform different alternative actions such as performing a man-in-the-middle attack or performing a phishing attack. The model in Figure 8 shows examples of subjective opinions associated with the six security events of the attack model. Table 2 presents the impact values of each security even, and Table 3 presents the effectiveness and cost of implementation of each countermeasure. To compute the impact at the top event node (data attack node) in Figure 12, we propagate the impact values given in Table 2 according to the set of propagation rules given in Table 1.

The subjective opinion about data attack is  $\langle 0.57, 0.18, 0.25, 0.76 \rangle$ , and the impact is 0.96. Therefore, the risk (as discussed in the preceding section) is approximated as a beta distribution with

Figure 8. The SAT model with countermeasures (ovals) for data attack example



**Table 2. The impact value of each attack in the data attack example**

Attack (security event)	Attack impact
Network scanning	0.2
Gaining access	0.5
Install zombie	0.6
Find vulnerable computers	0.8
Provoke the attack	0.6
Man in the middle	0.7
Phishing	0.4

**Table 3. The effectiveness and cost of implementation of each countermeasure in the data attack example**

Countermeasure	Countermeasure effectiveness	Countermeasure cost (in \$)
$CM_1$	0.80	15
$CM_2$	0.75	20
$CM_3$	0.60	10
$CM_4$	0.45	05

parameters  $\alpha = \langle 7.74, 2.86 \rangle$ . The mean of risk is 0.73, representing the most likely value of risk. The 95% confidence interval of the risk distribution is [0.30, 0.89], providing the lowest and highest possible values. Security managers here, in comparison to traditional risk assessment approaches, can use these values to reason about risk and make decisions as per their risk attitudes. Suppose, for example, that the security manager would only consider protection against the attack if the risk is greater than 0.5. Here, if they tend to use the most likely value (0.73) or if they are pessimistic regarding risk by considering the worst-case scenario (the risk value is 0.89), then they will go for protecting the system. However, considering the best-case scenario for those who tend to be optimistic regarding risk, they might go for not protecting the system as the value of risk considered in this case is only 0.30, which is below the defined threshold value. The consideration of uncertainty explicitly when conducting risk analysis, as this example demonstrates, offers therefore a better approach to decision-making by allowing one to consider different scenarios of risk and make decisions based on, for example, risk attitudes.

We now turn our attention to the analysis of security investments, using the ROI index. Applying each countermeasure would result in a reduction in the subjective opinion about the top event, i.e.,  $\omega_{goal}$ . Table 4 shows the subjective opinion about data attack when applying each countermeasure, as well as the percentage risk mitigated following uncertainty treatment using the most likely value approach. Using Equation 16, we obtain ROI for each countermeasure as shown in Table 4. As appear, two countermeasures,  $CM_1$  and  $CM_2$ , since their ROIs are negative, they should be excluded. The only two countermeasures that are profitable are  $CM_3$  and  $CM_4$ , and  $CM_3$  is more profitable than  $CM_4$ . However, ROI for  $CM_4$  approaches from zero, and so it does not seem to be significantly

Table 4. The subjective opinion on the root node, risk mitigated, and ROI for each countermeasure in the data attack scenario

Applied countermeasure	Subjective opinion on goal	Risk mitigated (%)	ROI
$CM_1$	$\langle 0.53, 0.20, 0.27, 0.75 \rangle$	4	-0.79
$CM_2$	$\langle 0.53, 0.20, 0.27, 0.75 \rangle$	4	-0.85
$CM_3$	$\langle 0.40, 0.36, 0.24, 0.62 \rangle$	28	1.13
$CM_4$	$\langle 0.52, 0.19, 0.29, 0.66 \rangle$	7	0.06

financially justified. As a result, the security manager may think of applying  $CM_3$  (authentication of the IP address) as a possible security solution against the attack.

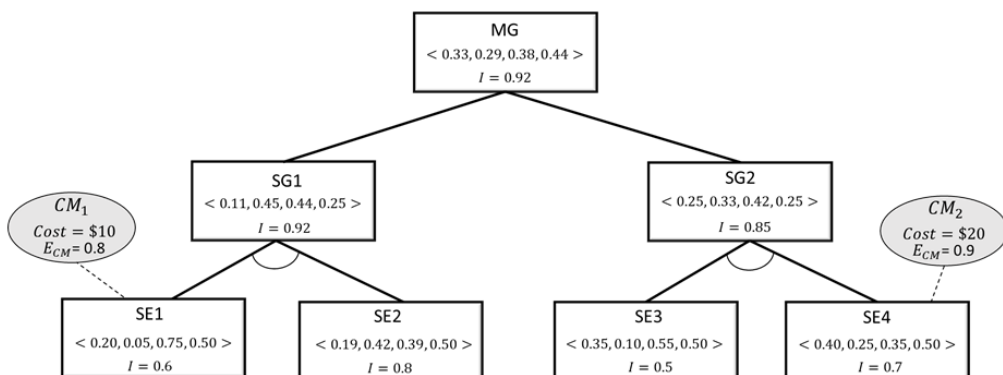
## COMPARISON WITH PROBABILISTIC ATS MODELS

In this section, we provide a detailed example to compare our approach against probabilistic ATs in terms of risk and security investments analysis. With the example, we aim to demonstrate why uncertainty about the probabilities of security events should be taken into account when conducting security risk analysis in ATs. Furthermore, we show how the decision-making process is better offered by the SAT model in comparison to traditional probabilistic ATs models. We begin by describing the comparison model, and then presenting and analysing the results.

### Comparison Model Description

We use the SAT model in Figure 9 as an example model to conduct the comparison. The model contains two countermeasures,  $CM_1$  (with a cost of \$10 and 0.8 effectiveness) and  $CM_2$  (with a cost of \$20 and 0.9 effectiveness), applied to the security events  $SE_1$  and  $SE_4$ , respectively. The subjective opinions about the four security events were established to contain relatively high uncertainty values. Propagating these opinions led to also having a relatively high uncertainty (0.38) about the likelihood on the root node.

Figure 9. A SAT model with two countermeasures. The values below the subjective opinions are impact values



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 could represent possible truth values for the subjective opinion about  $SE_4$  ( $\langle 0.40, 0.25, 0.35, 50 \rangle$ ). Here, the uncertainty value (0.35) has affected these probabilities as follows: it has affected only the belief mass of the probability distribution of 0.75 (because the sum of the uncertainty value and the belief mass of the opinion, i.e., 0.4, is 0.75), it has affected only the disbelief mass of the probability distribution of 0.6 (because the sum of the uncertainty value and the disbelief mass of the opinion (i.e., 0.25) is 0.6), and it has affected both the belief and disbelief masses of the probability distribution of 0.55 (here, the uncertainty has affected the belief mass by only 0.15).

Based on such a discussion, we generate probability values for the four security events in the example (assuming they represent truth values) as follows:  $Prob(SE_1) = 0.3$ ,  $Prob(SE_2) = 0.25$ ,  $Prob(SE_3) = 0.4$ , and  $Prob(SE_4) = 0.45$ . Here, we assumed that the uncertainties in the opinions about the security events had affected both the belief and disbelief masses of these probabilities at random. Propagating these probabilities, using the propagation method of probabilities discussed previously, resulting in a probability of 0.24 at the root node.

## Results and Analysis

First, we began by comparing the risk outcomes from the SAT model in Figure 9 with the risk obtained from applying traditional risk analysis using the above set of probabilities. In the case of the SAT model, the risk obtained is a beta distribution with parameters  $\alpha = \langle 2.92, 3.43 \rangle$  and mean 0.46. The 95% confidence interval of the risk distribution is [0.04, 0.74]. In the case of the AT approach, the risk obtained is a single value of 0.22. 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 the case of the AT approach, the system would not be protected. In the case of the SAT model, there are cases in which the security manager would choose to protect the system. For example, if the security manager tends to use the most expected value (i.e., the mean of risk), or if they are too pessimistic and wish to consider the worst-case scenario (via the upper bound of the confidence interval), they might go for protecting the system, as 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).

Next, we evaluated security investments (with ROI index) using the two models. In the SAT model, the subjective opinion about the attack without countermeasures is  $\langle 0.33, 0.29, 0.38, 0.44 \rangle$ . 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 5. Using this information

**Table 5. The projected probability of each subjective opinion about the attack with and without countermeasures and their 95% confidence intervals**

Protection status	Opinion on attack	Projected probability	95% Confidence interval
no protection	$\langle 0.33, 0.29, 0.38, 0.44 \rangle$	0.5	[0.29, 0.71]
with $CM_1$	$\langle 0.27, 0.32, 0.41, 0.26 \rangle$	0.37	[0.12, 0.61]
with $CM_2$	$\langle 0.14, 0.44, 0.42, 0.27 \rangle$	0.25	[0.03, 0.47]

and the cost of each countermeasure, we considered three scenarios for computing ROI for each countermeasure: (1) the most expected scenario (based on the projected probability), (2) the best-case scenario (based on the lower bound of the confidence interval), and (3) the worst-case scenario (based on the upper bound of the confidence interval). We denote the ROI calculated from the first scenario by  $ROI_{\mu}$ , and by  $ROI_{lower}$  and  $ROI_{upper}$  for the other two scenarios, respectively.

$ROI_{\mu}$  for  $CM_1$ , for example, is computed based on using the projected probability 0.37 (from the subjective opinion about the attack when presenting  $CM_1$ ) as a value for  $R_{sys}$  in Equation 16, and the percentage risk mitigated (%RM) is computed as  $1 - (0.37 / 0.5) = 0.26$ . Given that the cost of  $CM_1$  is \$10,  $ROI_{\mu}$  for  $CM_1$  is then  $((50 \times 0.26) - 10) / 10 = 0.3$ . The ROI values obtained for each countermeasure are all positives (except in one case) as shown in Table 6. In the case of AT model, the ROI obtained for each countermeasure, denoted by  $ROI_{pro}$ , is -0.49 for  $CM_1$  and -0.24 for  $CM_2$  (see Table 6). Clearly, none of the countermeasures is 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.

These results clearly demonstrate the importance of taking uncertainty into account when conducting cybersecurity risk assessments, as doing so can lead to completely different security decisions. In terms of the risk analysis, the SAT model offers a more flexible approach to decision-making by allowing one to consider different scenarios (e.g., the best and worst-case scenarios), and therefore allowing security managers to make decisions based on, for instance, their risk attitudes, or the organisation's financial capabilities. In terms of the security investments analysis (with ROI index), in addition to that the SAT model resulted in different ROI values for countermeasures, our example above interestingly showed that introducing uncertainty about the probabilities resulted 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 was higher, which might be also interpreted as follows: the SAT model in our example showed it is more inclined to protect the system in comparison to the traditional attack tree approach. To evaluate whether this observation generalises, more examples and analysis dealing with different sets of probabilities and different uncertainty values are required, which we leave for future work. For now, it has been clearly shown by the given example that the SAT model could result in different analysis of security investments, and therefore a different set of implementable countermeasures, demonstrating therefore the importance of considering uncertainty about the probabilities during security risk analysis.

**Table 6. ROI values for each countermeasure in the case of the SAT model ( $ROI_{\mu}$ ,  $ROI_{lower}$ , and  $ROI_{upper}$ ) and in case of AT approach ( $ROI_{pro}$ )**

Countermeasure	$ROI_{\mu}$	$ROI_{lower}$	$ROI_{upper}$	$ROI_{pro}$
$CM_1$	0.3	0.6	0	-0.49
$CM_2$	0.25	0.29	0.17	-0.24

## DISCUSSION

In this paper, we have presented a novel attack tree model, called a subjective attack tree (SAT), that takes second-order uncertainty into account, via subjective opinions. We also discussed the propagation rules of subjective opinion in the proposed model. Furthermore, we extended the SAT model to consider conducting a comprehensive security analysis, such as risk measuring and security investments analysis using ROI index. In the proposed SAT model, risk computation was discussed as one aspect of the security analysis. Since the probability component required to compute risk is not a single value, but rather a subjective opinion, the calculation of risk was different. We discussed how to compute risk (i.e., the expected impact) in case the impact is given as a single value in the range  $[0, 1]$  and in case it is represented as a beta distribution, demonstrating that in both representations of impact, the resulting value of risk is approximated as a beta distribution. It was therefore essential to also discuss how to understand risk as a beta distribution, and how to handle the uncertainty in the distribution for decision analysis.

Following this, we considered defence modelling, i.e., adding countermeasures to the model, to study how risk is reduced when adding them to a model containing uncertainty values about probabilities (i.e., subjective opinions). Here, because the nodes in our model contain subjective opinions (as likelihoods of attacks), adding a countermeasure to a node should affect the subjective opinion on it towards reducing its likelihood value, based on the effectiveness value of the countermeasure. We suggested that a countermeasure reduces (indirectly) the projected probability of the subjective opinion in the same way it does with probability values. To achieve this, we assumed that the effectiveness value of the countermeasure would affect only the belief mass and base rate while maintaining the same uncertainty value. This process ensures to have a subjective opinion that has a reduced projected probability according to the effectiveness value of the countermeasure.

Having incorporated countermeasures into the model, we discussed another aspect of security analysis, namely security investments analysis, using the index of ROI as a metric to measure the profitability of a given countermeasure. Classically, the formula for computing ROI for a countermeasure (see Equation 15) defines risk as a single value (because the probability and impact are assumed to be single values). In our model, the risk is beta distributed, and so we redefined the formula so as to capture the uncertainty aspect in likelihoods, discussing the difference in computing ROI in contrast to the computation in probabilistic models.

We discussed the importance and advantage of our approach in terms of risk and security investments analysis through a comparison model with the probabilistic approach. The results showed that risk analysis in SATs is different, and such a difference can lead to different security decisions. This is because that the uncertainty in the SAT model allows one to consider different scenarios for decision analysis, with which risk could be interpreted differently. Furthermore, regarding the security investments analysis, it has been shown that the SAT model resulted in different ROI values for countermeasures, and more interestingly, our example showed that these values were higher (in contrast to a 0 uncertainty). This means that the chance to apply a countermeasure in the SAT model was higher. To be able to evaluate whether this observation generalises, more examples and analysis dealing with different sets of probabilities and different uncertainty values are required, which we leave to future work.

## FUTURE WORK

In this section, we point out some future directions. In the section of security analysis using SATs, we used the index of ROI for security investment analysis (i.e., analysing the benefit from applying a particular countermeasure). Another index used in ATs aiming to analyse the gain from conducting

a particular attack is the *return on attack* (ROA; see Roy et al., 2012). It might be worth extending the security analysis by incorporating additional metrics, such as the cost of attack, allowing one to conduct ROA analysis (see Roy et al., 2012, Equation 14). First, the ROA formula needs to be redefined for the SAT model as we did with the ROI formula, and then use these defined formulas to quantify the nature of the competition between the attacker and the defender. One could also study how uncertainty about probabilities might affect such a competition, and how the best countermeasures can be selected under uncertainty about the two indexes.

Another future direction is more general that focuses on the possibility of extending the use of subjective logic to formalise other models of security risk analysis. Considering other models of security risk assessment, it might be worth examining how subjective logic could be used in these models to formalise the risk problem. For example, like attack trees, another model that is widely used to analyse risk of an enterprise network is *attack graphs* (Phillips & Swiler, 1998). In attack graphs, risk is analysed based on understanding how vulnerabilities can be combined and exploited to stage an attack. Traditionally, the composition of vulnerabilities can be modelled using probabilistic attack graphs (for example, see Feng & Jin-Shu, 2008; Keramati & Akbari, 2012; and L. Wang et al., 2008), which show all paths of attacks that will lead to network penetration. Using subjective logic, it might be possible to develop an alternative approach that measures security in absence of evidence about the vulnerability evaluations. Given that cycles could appear in attack graphs (as a result of the various ways that host interconnections and network privileges could be gained; see Homer et al., 2009), a key challenging may arise from the development of a subjective logic approach is that how to treat such cycles (to prevent distortion of the results) in the presence of uncertainty values about nodes probabilities.

## ACKNOWLEDGMENT

We thank the University of Technology and Applied Sciences (UTAS), Oman, for their unlimited support in making this research published. We also thank everyone who have had a direct or indirect hand in the successful completion of this research.

## COMPETING INTERESTS

The authors of this publication declare there are no competing interests.

## FUNDING AGENCY

This research was supported by the University of Technology and Applied Sciences (UTAS), Oman, as part of the Internal Funding Program.



## REFERENCES

- Al-Hadhrami, N., Collinson, M., & Oren, N. (2020). Security analysis using subjective attack trees. *Proceedings of the International Conference on Information Technology and Communications Security*, 288–301.
- Al-Hadhrami, N., Collinson, M., & Oren, N. (2021). Modelling security risk scenarios using subjective attack trees. *Proceedings of the 15th International Conference Crisis, 2020*, 201–218.
- Bistarelli, S., Fioravanti, F., & Peretti, P. (2006). Defense trees for economic evaluation of security investments. *Proceedings of the First International Conference on Availability, Reliability and Security*, 8. doi:10.1109/ARES.2006.46
- Bistarelli, S., Fioravanti, F., Peretti, P., & Santini, F. (2012). Evaluation of complex security scenarios using defense trees and economic indexes. *Journal of Experimental & Theoretical Artificial Intelligence*, 24(2), 161–192. doi:10.1080/13623079.2011.587206
- Buldas, A., Gadyatskaya, O., Lenin, A., Mauw, S., & Trujillo-Rasua, R. (2020). Attribute evaluation on attack trees with incomplete information. *Computers & Security*, 88, 101630. doi:10.1016/j.cose.2019.101630
- Buoni, A., Fedrizzi, M., & Mezei, J. (2010). A Delphi-based approach to fraud detection using attack trees and fuzzy numbers. *Proceedings of the International Association for the Scientific Knowledge (IASK) International Conferences*, 21–28.
- Cerutti, F., Kaplan, L., Kimmig, A., & Şensoy, M. (2019). Probabilistic logic programming with beta distributed random variables. *Proceedings of the Association for the Advancement of Artificial Intelligence (AAAI)*, 7769–7776. doi:10.1609/aaai.v33i01.33017769
- Couce-Vieira, A., Houmb, S. H., & Ríos-Insua, D. (2017). CSIRA: A method for analysing the risk of cybersecurity incidents. *Proceedings of the International Workshop on Graphical Models for Security*, 57–74.
- Daly, L. (1992). Simple SAS macros for the calculation of exact binomial and Poisson confidence limits. *Computers in Biology and Medicine*, 22(5), 351–361. doi:10.1016/0010-4825(92)90023-G PMID:1424580
- Edge, K., Raines, R., Grimaila, M., Baldwin, R., Bennington, R., & Reuter, C. (2007). The use of attack and protection trees to analyze security for an online banking system. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences*, 144b. doi:10.1109/HICSS.2007.558
- Edge, K. S., Dalton, G. C., Raines, R. A., & Mills, R. F. (2006). Using attack and protection trees to analyze threats and defenses to homeland security. *Proceedings of the 2006 IEEE Military Communications Conference*, 1–7. doi:10.1109/MILCOM.2006.302512
- Feng, C., & Jin-Shu, S. (2008). A flexible approach to measuring network security using attack graphs. *Proceedings of the 2008 International Symposium on Electronic Commerce and Security*, 426–431. doi:10.1109/ISECS.2008.122
- Gupta, A. K., & Nadarajah, S. (2004). *Handbook of beta distribution and its applications*. CRC Press. doi:10.1201/9781482276596
- Homer, J., Ou, X., & Schmidt, D. (2009). *A sound and practical approach to quantifying security risk in enterprise networks*. Kansas State University Technical Report.
- Jøsang, A. (2016). *Subjective logic*. Springer. doi:10.1007/978-3-319-42337-1
- Julious, S. A. (2005). Two-sided confidence intervals for the single proportion: comparison of seven methods by Robert G. Newcombe. *Statistics in Medicine*, 24(21), 3383–3384. doi:10.1002/sim.2164 PMID:16206245
- Julious, S. A. (2019). Calculation of confidence intervals for a finite population size. *Pharmaceutical Statistics*, 18(1), 115–122. doi:10.1002/pst.1901 PMID:30411472
- Jürgenson, A., & Willemson, J. (2007). Processing multi-parameter attack trees with estimated parameter values. *Proceedings of the International Workshop on Security*, 308–319.
- Kaplan, L., & Ivanovska, M. (2018). Efficient belief propagation in second-order Bayesian networks for singly connected graphs. *International Journal of Approximate Reasoning*, 93, 132–152. doi:10.1016/j.ijar.2017.10.031

- Keramati, M., & Akbari, A. (2012). An attack graph based metric for security evaluation of computer networks. *Proceedings of the 6th International Symposium on Telecommunications*, 1094–1098. doi:10.1109/ISTEL.2012.6483149
- Krichen, M., & Alroobaea, R. (2019, May). A new model-based framework for testing security of IoT systems in smart cities using attack trees and price-timed automata. *Proceedings of the 14th International Conference on Evaluation of Novel Approaches to Software Engineering*, 570–577. doi:10.5220/0007830605700577
- Kumar, R., & Stoelinga, M. (2017). Quantitative security and safety analysis with attack-fault trees. *Proceedings of the 2017 IEEE 18th International Symposium on High Assurance Systems Engineering*, 25–32. doi:10.1109/HASE.2017.12
- Lallemant, D., & Kiremidjian, A. (2015). A beta distribution model for characterizing earthquake damage state distribution. *Earthquake Spectra*, 31(3), 1337–1352. doi:10.1193/012413EQS013M
- Newcombe, R. G. (1998). Two-sided confidence intervals for the single proportion: Comparison of seven methods. *Statistics in Medicine*, 17(8), 857–872. doi:10.1002/(SICI)1097-0258(19980430)17:8<857::AID-SIM777>3.0.CO;2-E PMID:9595616
- Owen, C. E. B. (2008). *Parameter estimation for the beta distribution* [Master's thesis]. Brigham Young University. <http://hdl.lib.byu.edu/1877/etd2670>
- Phillips, C., & Swiler, L. P. (1998). A graph-based system for network vulnerability analysis. *Proceedings of the 1998 workshop on new security paradigms*, 71–79. doi:10.1145/310889.310919
- Pieters, W., & Davarynejad, M. (2014). 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.
- Roy, A., Kim, D. S., & Trivedi, K. S. (2010). Cyber security analysis using attack countermeasure trees. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research*, 1–4. doi:10.1145/1852666.1852698
- Roy, A., Kim, D. S., & Trivedi, K. S. (2012). Attack countermeasure trees (ACT): Towards unifying the constructs of attack and defense trees. *Security and Communication Networks*, 5(8), 929–943. doi:10.1002/sec.299
- Scala, N. M., Goethals, P. L., Dehlinger, J., Mezgebe, Y., Jilcha, B., & Bloomquist, I. (2022). Evaluating mail-based security for electoral processes using attack trees. *Risk Analysis*, 42(10), 2327–2343. doi:10.1111/risa.13876 PMID:35072977
- Schneier, B. (1999). Attack trees. *Dr. Dobbs's Journal*, 24(12), 21–29.
- Shang, W., Gong, T., Chen, C., Hou, J., & Zeng, P. (2019). Information security risk assessment method for ship control system based on fuzzy sets and attack trees. *Security and Communication Networks*, 2019, 3574675. doi:10.1155/2019/3574675
- Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI): A practical quantitative model. *Journal of Research and Practice in Information Technology*, 38(1), 45.
- Valluripally, S., Gulhane, A., Mitra, R., Hoque, K. A., & Calyam, P. (2020, January). Attack trees for security and privacy in social virtual reality learning environments. *Proceedings of the 2020 IEEE 17th Annual Consumer Communications and Networking Conference*, 1–9. doi:10.1109/CCNC46108.2020.9045724
- Wang, L., Islam, T., Long, T., Singhal, A., & Jajodia, S. (2008). An attack graph-based probabilistic security metric. *Proceedings of the IFIP Annual Conference on Data and Applications Security and Privacy*, 283–296.
- Wang, P., Lin, W.-H., Kuo, P.-T., Lin, H.-T., & Wang, T. C. (2012). Threat risk analysis for cloud security based on attack-defense trees. *Proceedings of the 8th International Conference on Computing Technology and Information Management*, 1, 106–111.
- Zhang, Q., Zhou, C., Tian, Y.-C., Xiong, N., Qin, Y., & Hu, B. (2017). A fuzzy probability Bayesian network approach for dynamic cybersecurity risk assessment in industrial control systems. *IEEE Transactions on Industrial Informatics*, 14(6), 2497–2506. doi:10.1109/TII.2017.2768998

*Nasser Al-Hadhrani is a Senior Lecturer at the University of Technology and Applied Sciences (UTAS), Oman. Nasser achieved his PhD in Computing Sciences in 2021 from the University of Aberdeen, UK. He obtained his Master's degree in 2014 from the University of Portsmouth (UK) in the field of Cybersecurity. Before joining UTAS, Nasser was working as a Lecturer at the University of Nizwa, Oman, and before this, he had been working as a teacher in the Ministry of Education. Nasser has research interests in the domains of Cyber security and Artificial Intelligence. Mainly, he is interested in the topics of computer and network security, formal methods, and AI in security and security in AI.*