Belief-Based Risk Analysis

Audun Jøsang[1] **Daniel Bradley**[2] **Svein J. Knapskog**[3]

[1]Distributed Systems Technology Centre*
UQ Qld 4072, Australia
Email: ajosang@dstc.edu.au

[2]Securizance, Brisbane, Australia
Email: daniel.bradley@securizance.com

[3]Department of Telematics, Norwegian University of Science and Technology
N-7491 Trondheim, Norway
Email: svein.knapskog@item.ntnu.no

Abstract

This paper describes a method for risk analysis based on the approach used in CRAMM, but instead of using discrete measures for threats and vulnerabilities and look-up tables to derive levels of risk, it uses subjective beliefs about threats and vulnerabilities as input parameters, and uses the belief calculus of subjective logic to combine them. Belief calculus has the advantage that uncertainty about threat and vulnerability estimates can be taken into consideration, and thereby reflecting more realistically the nature of such estimates. As a result, the computed risk assessments will better reflect the real uncertainties associated with those risks.

Keywords: Security, risk analysis, belief calculus

1 Introduction

When security is to be included in IT system, a risk analysis provides a systematic method for defining the security requirements. A logical approach to risk analysis is first to get an overview of all the assets, to determine all possible threats and to identify the vulnerabilities. From this, the risk analysis must try to determine potential direct negative impact on assets, and finally the consequences this can have on the organisation.

In this paper we will interpret a *threat* as something (e.g. persons, groups or activities) that tries to cause security incidents on assets. We will use the term *asset impact* to denote a security incident affecting a particular asset. An asset can be anything that has a value to an organisations (e.g. IT systems, information, staff, reputation, goodwill), and the *impact cost* is the estimated cost to the organisation resulting from the direct damage to the asset and from any negative consequences on the organisation in case an asset impact occurs. *Vulnerability* is defined as the lack of protection (e.g no firewalls, poor passwords, presence of software security flaws) against threats against assets. The likelihood of an asset impact can be determined as the "product" of the threat against that asset and its vulnerability. The risk can then be determined as the "product" of the likelihood of an asset impact and the impact cost. This is in line with the approach taken by CRAMM(CCTA 1991) which is a well known typical risk management methodology where threats, vulnerabilities and asset values are quantified as discrete measures. The basic principles of CRAMM are explained in Sec.3 below.

Risk resolution consists of determining the most suitable countermeasures to reduce the vulnerability and thereby the risk. Together, risk analysis and risk resolution can be called risk management. Our approach extends the methodology used in CRAMM by quantifying threats and vulnerabilities as beliefs, and impact costs in dollars and cents. We then show how the risk analysis part can be enhanced by using belief calculus operators from subjective logic(Jøsang 2001, Jøsang 2002, Jøsang & Grandison 2003) for analysing these beliefs and for combining the results with impact costs.

2 The Belief Model

2.1 Representing Beliefs

Belief calculus is suitable for approximate reasoning in situations where there is more or less uncertainty about whether a given proposition is true or false, and this uncertainty can be expressed by a belief mass assignment[1] (BMA) where a quantity of belief mass on a given proposition can be interpreted as contributing to the probability that the proposition is true.

More specifically, if a set denoted by Θ of exhaustive mutually exclusive atomic elements can be defined, this set is referred to as a frame of discernment. Each atomic element can be interpreted as a proposition that can be either true or false. The powerset of Θ denoted by 2^Θ contains all possible subsets of Θ. The set $2^\Theta - \{\emptyset\}$ of nonempty subsets of Θ will be called its reduced powerset. A BMA assigns belief mass to nonempty subsets of Θ (*i.e.* to elements of $2^\Theta - \{\emptyset\}$) without specifying any detail of how to distribute the belief mass amongst the elements of a particular subset (or even among its nontrivial subsets). In this case, then for any nontrivial subset of Θ, a belief mass on that subset expresses uncertainty regarding the probability distribution over the elements of the subset. More generally, a belief mass assignment m on Θ is defined as a function from $2^\Theta - \{\emptyset\}$ to $[0, 1]$ satisfying:

$$\sum_{x \subseteq \Theta} m(x) = 1. \quad (1)$$

Each nonempty subset $x \subseteq \Theta$ such that $m(x) > 0$ is called a focal element of m. A *vacuous* BMA is when $m(\Theta) = 1$ whereas a *dogmatic* BMA is when $m(\Theta) = 0$. Given a particular frame of discernment and a BMA, the Dempster-Shafer theory (Shafer 1976) defines a belief

*The work reported in this paper has been funded in part by the Co-operative Research Centre for Enterprise Distributed Systems Technology (DSTC) through the Australian Federal Government's CRC Programme (Department of Industry, Science & Resources).

[1]Called *basic probability assignment* in (Shafer 1976).

function[2] $b(x)$. In addition, subjective logic (Jøsang 2001) defines a disbelief function $d(x)$, an uncertainty function $u(x)$, a relative atomicity function $a(x/y)$ and a probability expectation $\mathrm{E}(x)$. These are all defined as follows:

$$b(x) \triangleq \sum_{\emptyset \neq y \subseteq x} m(y) \qquad \forall\, x \in 2^{\Theta}\,, \qquad (2)$$

$$d(x) \triangleq \sum_{y \cap x = \emptyset} m(y) \qquad \forall\, x \in 2^{\Theta}\,, \qquad (3)$$

$$u(x) \triangleq \sum_{\substack{y \,\cap\, x \,\neq\, \emptyset \\ y \,\not\subseteq\, x}} m(y) \qquad \forall\, x \in 2^{\Theta}\,, \qquad (4)$$

$$a(x/y) \triangleq \frac{|x \cap y|}{y} \qquad \forall\, x \in 2^{\Theta}\,, \qquad (5)$$

$$\mathrm{E}(x) \triangleq \sum_{y \subseteq \Theta} m_{\Theta}(y)\, a(x/y) \qquad \forall\, x \in 2^{\Theta}\,. \qquad (6)$$

The relative atomicity function of a subset x relative to the frame of discernment Θ is simply denoted by $a(x)$.

Subjective logic applies to binary frames of discernment, so in case a frame is larger than binary, a coarsening is required to reduce its size to binary. Coarsening focuses on a particular subset $x \subset \Theta$, and produces a binary frame of discernment X containing x and its complement $\overline{x}$. The powerset of X is $2^X = \{x, \overline{x}, X\}$ which has $2^{|X|} - 1 = 3$ elements when excluding $\emptyset$. The coarsening process also produces belief, disbelief, uncertainty, and relative atomicity functions for the element x in focus. Let the coarsened frame of discernment be $X = \{x, \overline{x}\}$ where $\overline{x}$ is the complement of x in Θ. We will denote by b_x, d_x, u_x and a_x the belief, disbelief, uncertainty and relative atomicity functions of x on X.

Different types of coarsening are possible. In *simple coarsening*(Jøsang 2001) the belief, disbelief and uncertainty functions on x in X are identical to those in Θ. The simple relative atomicity function on the other hand produces a synthetic relative atomicity value which does not represent the real relative atomicity of x on Θ in general. However the probability expectation value of x is equal in Θ and X, as expected.

In *normal coarsening*(Jøsang & Grandison 2003) the relative atomicity function represents the actual relative atomicity of x on Θ. The relative cardinality of an element in a binary frame of discernment will always be 0.5, whereas the normal relative atomicity reflects the true relative atomicity of an element relative to the original frame of discernment.

An opinion ω_x held by an individual about a proposition x is the ordered quadruple (b_x, d_x, u_x, a_x). Note that b_x, d_x, u_x and a_x must all fall in the closed interval $[0, 1]$, and $b_x + d_x + u_x = 1$. For both simple and normal coarsening, the expected probability for x satisfies $\mathrm{E}(\omega_x) \triangleq \mathrm{E}(x) = b_x + a_x u_x$. Although the coarsened frame of discernment X is binary, an opinion about $x \in X$ carries information about the state space size of the original frame of discernment Θ through the relative atomicity parameter a_x.

The opinion space can be mapped into the interior of an equal-sided triangle, where, for an opinion $\omega_x = (b_x, d_x, u_x, a_x)$, the three parameters b_x, d_x and u_x determine the position of the point in the triangle representing the opinion. Fig.1 illustrates an example where the opinion about a proposition x from a binary frame of discernment has the value $\omega_x = (0.7,\ 0.1,\ 0.2,\ 0.5)$.

The top vertex of the triangle represents uncertainty, the bottom left vertex represents disbelief, and the bottom right vertex represents belief. The parameter b_x is the value of a linear function on the triangle which takes value 0 on the edge which joins the uncertainty and disbelief vertices and takes value 1 at the belief vertex. In other words, b_x is equal to the quotient when the perpendicular distance between the opinion point and the edge joining the uncertainty and disbelief vertices is divided by the perpendicular distance between the belief vertex and the same edge. The parameters d_x and u_x are determined similarly. The edge joining the disbelief and belief vertices is called the probability axis. The relative atomicity is indicated by a point on the probability axis, and the projector starting from the opinion point is parallel to the line that joins the uncertainty vertex and the relative atomicity point on the probability axis. The point at which the projector meets the probability axis determines the expectation value of the opinion, *i.e.* it coincides with the point corresponding to expectation value $b_x + a_x u_x$.

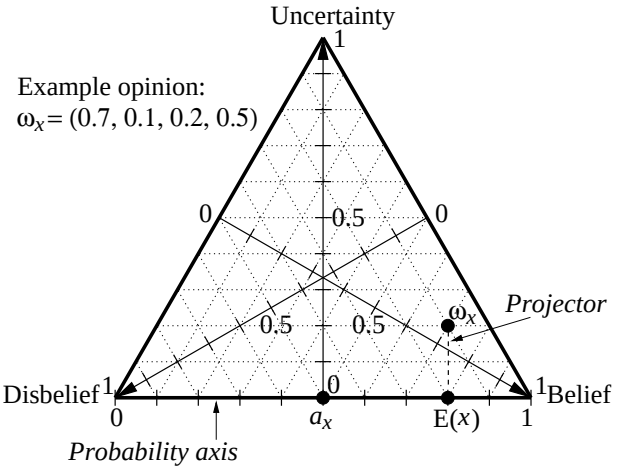

Figure 1: Opinion triangle with example opinion

Opinions can be ordered according to probability expectation value, but additional criteria are needed in case of equal probability expectation values. We will use the following rules to determine the order of opinions(Jøsang 2001):

Let ω_x and ω_y be two opinions. They can be ordered according to the following rules by priority:

1. The opinion with the greatest probability expectation is the greatest opinion.
2. The opinion with the least uncertainty is the greatest opinion.
3. The opinion with the least relative atomicity is the greatest opinion.

Opinions can be expressed as beta pdfs (probability density functions) denoted by beta (α, β) through the following mapping:

$$\begin{aligned} &(b_x, d_x, u_x, a_x) \longmapsto \\ &beta\left(\tfrac{2b_x}{u_x} + 2a_x,\ \ \tfrac{2d_x}{u_x} + 2(1 - a_x)\right). \end{aligned} \qquad (7)$$

This means for example that an opinion with $u_x = 1$ and $a_x = 0.5$ which maps to *beta* $(1, 1)$ is equivalent to a uniform pdf. It also means that a dogmatic opinion with $u_x = 0$ which maps to *beta* $(b_x\eta,\ d_x\eta)$ where $\eta \to \infty$ is equivalent to a spike pdf with infinitesimal width and infinite height. Dogmatic opinions can thus be interpreted as being based on an infinite amount of evidence.

2.2 Reasoning with Beliefs

Subjective logic defines a number of operators. Some operators represent generalisations of binary logic and probability calculus whereas others are unique are unique to belief theory because they depend on belief ownership.

[2] Denoted by $Bel(x)$ in (Shafer 1976).

Table 1: Belief operators in subjective logic

Belief operator name	Opinion operator symbol	Logic operator symbol	Logic operator name
Multiplication	$\omega_x \cdot \omega_y$	$x \wedge y$	AND
Division	ω_x / ω_y	$x \overline{\wedge} y$	UN-AND
Comultiplication	$\omega_x \sqcup \omega_y$	$x \vee y$	OR
Codivision	$\omega_x \overline{\sqcup} \omega_y$	$x \overline{\vee} y$	UN-OR
Complement	$\neg \omega_x$	$\overline{x}$	NOT
Discounting	$\omega_B^A \otimes \omega_x^B$	$A : B : x$	SERIAL TRANSITIVITY
Consensus	$\omega_x^A \oplus \omega_x^B$	$(A, B) : x$	PARALLEL COMBINATION
Conditional inference	$\omega_x \circledcirc (\omega_{y\|x}, \omega_{y\|\overline{x}})$	$y \| x$	MODUS PONENS

Multiplication[3] is equivalent to multiplication of probabilities in case of dogmatic opinions, and to binary logic AND in case of absolute opinions (Jøsang 2001, Jøsang & McAnally 2004). Division is equivalent to division of probabilities in case of dogmatic opinions, and to binary logic UN-AND in case of absolute opinions (Jøsang & McAnally 2004).

Comultiplication[4] is equivalent to comultiplication of probabilities in case of dogmatic opinions, and to binary logic OR in case of absolute opinions (Jøsang 2001, Jøsang & McAnally 2004). Codivision is equivalent to codivision of probabilities in case of dogmatic opinions, and to binary logic UN-OR in case of absolute opinions (Jøsang & McAnally 2004).

Complement[5] is equivalent to complement of probabilities in case of dogmatic opinions, and to binary logic NOT in case of absolute opinions.

Discounting does not have any equivalent operator in probability calculus or binary logic. Discounting is used to compute transitive trust, i.e. if Alice trusts Bob, and Bob trusts Clark, and Bob recommends Clark to Alice, then Alice will discount the recommendation as a function of her trust in Bob. The effect of discounting in a transitive chain is that uncertainty increases (and not disbelief) (Jøsang, Gray & Kinateder 2003).

Consensus is equivalent to Bayesian update in probability calculus. However there is no corresponding binary logic operator (Jøsang 2002) because that would be the same as trying to combine contradictory statements such as for example combining x with NOT x. This is in fact perfectly possible in subjective logic(Jøsang, Daniel & Vannoorenberghe 2003).

The Subjective Logic API (SL-API) is a Java implementation of the operators in Table 1.

3 Risk Analysis with CRAMM

The acronym CRAMM(CCTA 1991) stands for CCTA[6] Risk Analysis and Management Methodology. The method for risk analysis used by CRAMM and most other methodologies consists of evaluating the following three factors:

- the threats that can affect that asset, and
- the vulnerabilities that can be exploited by a threat,
- the cost in case of impact on an asset

and from this determine a risk level or establish some measure of risk. This is conceptually illustrated in Fig.2.

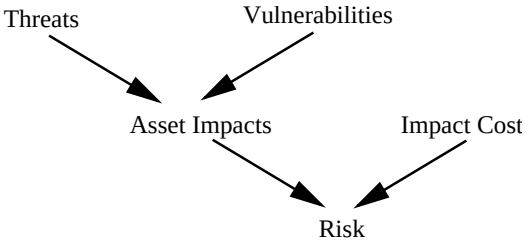

Figure 2: Conceptual illustration of risk analysis

The risk analysis itself consists of five parts:

1. **Identify assets, threats and vulnerabilities**.
   Each potentially impacted asset must be identified. Lists of all imaginable threats, of all relevant vulnerabilities, and of all potentially affected assets are established.

2. **Identify potential asset impacts.**
   A list of all combinations of threat and a vulnerabilities which potentially can cause an impact on an asset are identified. This is illustrated in Fig.3.

3. **Value assets and measure threats and vulnerabilities.**
   Each potentially affected asset must be valued according to the cost of loss or damage of the asset. All values are transcribed into a scale from 1 to 10. The strength of the threats and the level of the vulnerabilities must be quantified. Possible values for both threat and vulnerability are *low*, *medium* and *high*.

4. **Calculate the risk.**
   A fixed 3 dimensional lookup table (Tab.2) where the strength of the threat, the level of the vulnerability and the value of the asset are input parameters, gives the final security requirement (= risk) in the range 1 through 5.

5. **Review the results.**
   At this point it is useful to review the data. A bit of common sense must be used to see if the results seem reasonable. Usually, an adjustment of the input data is needed.

After the risk analysis, suitable countermeasures can be selected, and the risk analysis can eventually be done again with the countermeasures included, in order to see whether the risk has been reduced to an acceptable level.

[3] Called "propositional conjunction" in (Jøsang 2001).

[4] Called "propositional disjunction" in (Jøsang 2001).

[5] Called "negation" in (Jøsang 2001).

[6] Originally, CCTA stood for *Central Computer and Telecommunications Agency*. The actual name is *The Government Center for Information Systems*. It is a branch of the Treasury Department in the UK, and they give advice on computer security among other things.

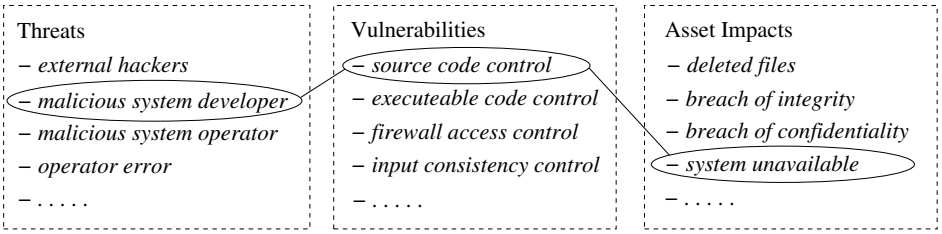

Figure 3: Potential impacts: Combinations of threat, vulnerability and impact

Table 2: CRAMM risk look-up matrix

Threat rating	low			medium			high		
Vulnerability	l	m	h	l	m	h	l	m	h
Asset value									
1	1	1	1	1	1	1	1	1	2
2	1	1	1	1	1	1	1	1	2
3	1	1	2	1	2	2	2	2	3
4	1	2	2	2	2	3	3	3	4
5	2	2	3	2	3	3	3	3	4
6	2	3	3	3	3	4	3	4	4
7	3	3	4	3	4	4	4	4	5
8	3	4	4	4	4	5	4	5	5
9	4	4	5	4	5	5	5	5	5
10	4	5	5	5	5	5	5	5	5

4 Risk Analysis using Subjective Logic

4.1 Informal Description

A CRAMM like methodology can be made more general and flexible using subjective logic. Opinions are suitable to quantify threats and vulnerabilities due to the possibility of including the ignorance which always is present when making such assessments. Opinions regarding impacts can be obtained by combining opinions about threats and vulnerabilities by multiplication. Finally, the impact cost can be seen as a factor associated with each asset impact so that a risk for each asset impact can be computed as the product of the probability expectation value of the asset impact and the impact cost. The risks can be ordered and graphically represented for example as beta pdfs in order to provide a visual representation of risks.

4.2 Formalising Risk Analysis

Let the threats be denoted by T_i where the index i indicates the the threat type, let the vulnerabilities be denoted by V_j where the index j indicates the vulnerability type, and let the assets impacts be denoted by AI_k where the indexed k indicates the asset impact type. Each valid combination of threat, vulnerability and asset impacts will be denoted by $\mathrm{T/V/AI}/_l$ where index l indicates the the particular valid combination.

The opinion about a valid T/V/AI combination can then be expressed as:

$$\omega_{\mathrm{T/V/AI}_l} = \omega_{\mathrm{T}_i} \cdot \omega_{\mathrm{V}_j} \tag{8}$$

The mapping from opinions to beta pdfs defined by Eq.(7) allows the above opinion to be expressed as a beta pdf denoted by $beta_{\mathrm{T/V/AI}_l}$. We will use the beta pdf representation in order to visualise the risk in a 3D diagram. The SL-API[7] was used for the belief computations in the example below. Gnuplot was used to draw the graphs.

[7] Available at: http://security.dstc.edu.au/spectrum/sl-api/

4.3 Numerical Example

Let the opinions about threats and vulnerabilities be defined according to Table 3 and Table 4.

Table 3: Example opinions about threats

T	Threat	Opinion
1	external hacker	(0.90, 0.05, 0.05, 0.5)
2	malicious developer	(0.08, 0.80, 0.12, 0.5)
3	malicious operator	(0.03, 0.90, 0.07, 0.5)
4	operator error	(0.20, 0.75, 0.05, 0.5)

In modern risk analysis methodologies the list of threats can contain several hundred different types of threats, and in our example we have only included four types in the list above. Similarly, the list of vulnerabilities can contain several hundred different types, and we have only included four types in the list below.

Table 4: Example opinions about vulnerabilities

V	Vulnerability	Opinion
1	source code control	(0.60, 0.35, 0.05, 0.5)
2	executable code control	(0.05, 0.90, 0.05, 0.5)
3	firewall access control	(0.01, 0.95, 0.04, 0.5)
4	input data control	(0.10, 0.80, 0.10, 0.5)

A combination of threat and vulnerability can impact specific assets, and the list of different assets can be quite large. For the purpose of this example we have only included four different asset impacts and their costs in Table 5 below.

Table 5: Example asset impacts and costs

AI	Asset Impact	Impact Cost
1	deleted files	$ 1,000,000
2	breach of integrity	$ 200,000
3	breach of confidentiality	$ 100,000
4	system unavailable	$ 500,000

We now define the valid combinations of threats, vulnerabilities and asset impacts from Tables 3, 4 and 5 and compute the opinions of the combinations according to Eq.(8). We also convert each opinion into a beta pdf according to Eq.(7). A beta pdf represents the probability density function of the likelihood of an asset impact to occur as a function of the relevant threat and vulnerability combination. These results are summarised in Table 6. The list of valid combinations is not supposed to be a realistic exhaustive list of possible impact combinations.

We are then able to illustrate the probabilities of valid T/V/AI combinations as beta pdfs, see Fig.4.

Table 6: Example valid combinations of threats, vulnerabilities and asset impacts

T/V/AI combination	T	V	AI	Opinion about T/V/AI combination	Beta pdf of T/V/AI combination	Impact Cost
1	1	3	3	(0.021, 0.952, 0.026, 0.250)	beta(2.1, 74.7)	$ 100,000
2	2	1	1	(0.073, 0.870, 0.057, 0.250)	beta(3.1, 32.0)	$ 1,000,000
3	2	1	3	(0.073, 0.870, 0.057, 0.250)	beta(3.1, 32.0)	$ 100,000
4	2	1	4	(0.073, 0.870, 0.057, 0.250)	beta(3.1, 32.0)	$ 500,000
5	3	4	2	(0.006, 0.980, 0.014, 0.250)	beta(1.4, 141.5)	$ 200,000
6	3	4	3	(0.006, 0.980, 0.014, 0.250)	beta(1.4, 141.5)	$100,000
7	4	4	1	(0.025, 0.940, 0.035, 0.250)	beta(1.9, 55.2)	$1,000,000
8	4	4	2	(0.025, 0.940, 0.035, 0.250)	beta(1.9, 55.2)	$200,000

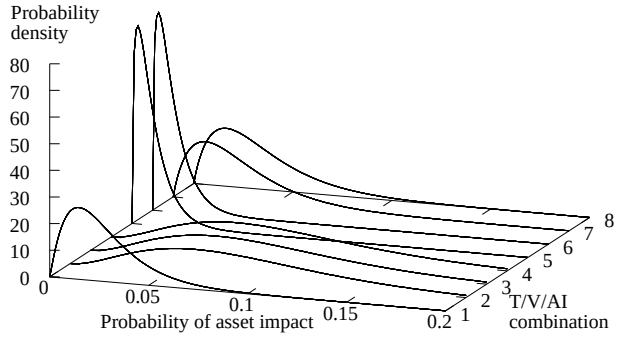

Figure 4: Visualisation of asset impact likelihood

The probability densities over asset impact probabilities are concentrated close to zero on the X-axis, so the X-axis therefore only covers the range [0.0, 0.2]. High density close to zero on the X-axis means that the likelihood (i.e. expected probability) of asset impact is low. The likelihood of asset impact increases when the density flows into higher values on the X-axis.

Some T/V/AI combinations have identical pdfs because they result from the same T/V pair without taking the AI cost into account. Fig.4 thus only represents the likelihood of an asset impact to occur, and does not indicate the risk involved.

In order to illustrate how uncertain levels of risk can be derived, each AI probability can be multiplied with the corresponding impact cost, so that the X-axis now represents impact cost. A pdf over impact costs can be interpreted as risk. The pdfs of impact costs will be stretched along the X-axis as a function of the nominal value of the corresponding impact cost. This is illustrated in Fig.5.

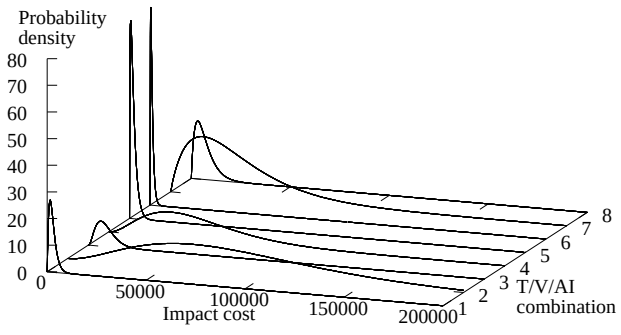

Figure 5: Visualisation of risk as pdfs over impact cost

The densities are concentrated close towards zero value on the X-axis, so that the X-axis only covers the range [$0, $200,000] although the highest impact cost actually is $1,000,000. The densities towards $1,000,000 are only infinitesimal so that it would not be interesting to illustrate them.

The closer to zero the density is concentrated, the less the risk. The more the density is spread out over higher impact costs (towards the right side) then the higher the risk. In this way it is easy to get an impression of the risk level for each T/V/AI combination. It can be seen that T/V/AI combinations 2, 4 and 7 have their risk densities more spread out than the other combinations.

The probability expectation value of each T/V/AI combination can be computed with Eq.(6). When multiplying the probability expectation value with the impact cost, the expected risk can be computed. These results are summarised in Table 7 below.

Table 7: Expectation values for asset impact probability and risk

T/V/AI combination	Asset Impact probability expectation	Expected Risk
1	0.02750	$ 2,750
2	0.08725	$ 87,250
3	0.08725	$ 8,725
4	0.08725	$ 43,625
5	0.00950	$ 1,900
6	0.00950	$ 950
7	0.03375	$ 33,750
8	0.03375	$ 6,750

It can be seen that T/V/AI combination 2 has the highest expected risk, followed by T/V/AI combinations 4 and 7, as already indicated by Fig.5.

Whenever the same asset impact is involved in different T/V/AI combinations, the corresponding risk for that asset impact could be computed by combining all valid combinations of threats and vulnerabilities that can have the same asset impact. This would translate into comultiplication of the opinions about those combinations so that for example the opinion about AI_1 ("deleted files") could be computed by comultiplying the opinions about T/V/AI combinations 2 and 7 from Table 6 as:

$$\omega_{\mathrm{AI}_1} = (\omega_{\mathrm{T}_2} \cdot \omega_{\mathrm{V}_1}) \sqcup (\omega_{\mathrm{T}_4} \cdot \omega_{\mathrm{V}_4}) \quad (9)$$

However, whenever there is dependence between different combinations this method will not give correct result. That is the reason why we chose to compute the risk of each combination separately, so that the same asset impact may occur in several rows in Table 6.

5 Conclusion

Ignorance is not properly accounted for in traditional mathematical reasoning frameworks such as binary logic and probability calculus. When risk analysis is based on such calculi, it will not be able to reflect that the results also are partly ignorant, and thereby gives a false picture

of a system's security state. We have described how risk analysis can be implemented with subjective logic which has the advantage of enabling ignorance into to be taken into consideration. The results of the risk analysis are then easy to interpret and clearly show the degree of ignorance it contains.

The main difficulty when performing a risk analysis is to properly determine the input parameters, which in our model are the subjective opinions about threats and vulnerabilities and the impact costs. If the evidence at hand can be analysed statistically, Bayesian updating can be used. If on the other hand the evidence can only be analysed intuitively, we believe that guidelines can be useful in order to get as uniform and consistent opinions as possible. The problem of defining input parameters will nevertheless remain the weakest point in any risk analysis methodology.

References

CCTA (1991), *CRAMM User's Guide (Version 2.0)*, The UK Central Computer and Telecommunications Agency.

Jøsang, A. (2001), 'A Logic for Uncertain Probabilities', *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* **9**(3), 279–311.

Jøsang, A. (2002), 'The Consensus Operator for Combining Beliefs', *Artificial Intelligence Journal* **142**(1–2), 157–170.

Jøsang, A., Daniel, M. & Vannoorenberghe, P. (2003), Strategies for Combining Conflicting Dogmatic Beliefs, *in* X. Wang, ed., 'Proceedings of the 6th International Conference on Information Fusion'.

Jøsang, A. & Grandison, T. (2003), Conditional Inference in Subjective Logic, *in* X. Wang, ed., 'Proceedings of the 6th International Conference on Information Fusion'.

Jøsang, A., Gray, E. & Kinateder, M. (2003), Analysing Topologies of Transitive Trust, *in* 'Proceedings of the Workshop of Formal Aspects of Security and Trust (FAST 2003)'.

Jøsang, A. & McAnally, D. (2004), 'Multiplication and Comultiplication of Beliefs (*to appear*)', *International Journal of Approximate Reasoning* .

Shafer, G. (1976), *A Mathematical Theory of Evidence*, Princeton University Press.