19

Checklist-Based Risk Analysis with Evidential Reasoning

Sungbaek Cho and Zbigniew Ciechanowicz
Information Security Group, Royal Holloway College, University of London, Egham, Surrey, TW20 0EX, UK

Key words: Risk Analysis, Checklist, Belief Function, Evidential Network, BS7799

Abstract: Measuring risk is not a simple task since it almost invariably includes an analyst's subjective judgment. Risk analysis often forces the analyst to estimate or predict future events, which are uncertain. Therefore, we should consider the uncertainties associated with judgments made by the analyst. Hence in this article, we try to apply belief functions, which are used to express and manipulate uncertainties. We use an evidential network to combine answers and uncertainties from a checklist-based risk analysis. A checklist method is still useful in that it is relatively easier and simpler than other risk analysis methods. Furthermore, a checklist-based risk analysis can be used in a baseline approach. To establish the measure of risk in a checklist-based analysis, and the uncertainty that exists in this measurement, we suggest the use of belief functions. An evidential network deployed in a checklist-based risk analysis can also be applied to the self-assessment of BS7799 compliance when preparing for accredited certification against BS7799.

1. INTRODUCTION

Risk analysis is a useful tool for organisations in identifying possible security holes in information systems and providing appropriate countermeasures against them. Risk analysis is, by definition in ISO/IEC TR13335-1 (1996), the process of identifying security risks, determining their magnitude, and identifying areas that need safeguards. Risk analysis is an essential tool for systematic management of information security as it is used in identifying the potential risks and providing useful information to

management for planning and organising security. Pfleeger (1997) argues that there are several benefits of risk analysis such as improved awareness of security, identification of assets, threats and vulnerabilities and improved decision basis for security investment. However, he also points out that the problems in risk analysis, such as imprecise inputs, too much focus on numeric values, and users' tendency to use the same inputs over several years, are the factors that bring into doubt the value of risk analysis. These problems are not just restricted to information security risk assessment, but are equally valid in any complex and unstructured decision making situation. Within risk management, risk analysis is regarded as the point where most difficulty arises (Rainer, et al. 1991).

Besides the methodological difficulties in measuring risk, the other concern is that formal risk analysis can be a time-consuming and expensive process (Erwin1994). Formal risk analysis includes the identification and valuation of assets, threats and vulnerabilities, as detailed in ISO/IEC TR 13335-3 (1997). However, it is equally true that risk analysis is critical for preserving security and the benefits of a well-performed risk analysis far outweigh any drawbacks (Ciechanowicz 1997). From the viewpoint of level of detail and granularity of risk analysis, methods are mainly classified into four categories (ISO/IEC TR 13335-2 1997): (1) baseline approach, (2) informal approach, (3) detailed risk analysis and (4) combined approach. In the baseline approach, a standard set of safeguards is applied to all information systems so as to achieve a baseline level of protection. In an informal approach, we conduct a pragmatic risk analysis on all systems by exploiting the knowledge and experience of security professionals. Detailed risk analysis refers to the detailed review of systems, which includes the identification and valuation of assets, and assessment of the levels of threats to those assets and associated vulnerabilities. The combined approach balances the baseline and detailed approaches by applying detailed risk analysis to important systems while protecting less important systems with a baseline approach. ISO/IEC TR 13335-3 (1997) recommends the use of the combined approach for efficient and effective allocation of organisational resources for risk analysis.

2. CHECKLIST METHOD AND BASELINE APPROACH

Owing to the critical role of risk analysis in security management, a number of risk analysis methods have been developed since the early 1980s. Examples include CRAMM (CCTA Risk Analysis and Management Method, CCTA 1990), annualised loss expectancy (ALE), Courtney, the

Livermore Risk Analysis Method (LRAM), Stochastic Dominance, Checklist, and Fuzzy metrics. An overview of these methods is well summarised in Rainer, et al. (1991).

In this article, our interest is in checklist-based risk analysis. Checklist method (also known as a simple questionnaire method) uses a series of questions to assess risk. There are a number of sources that provide security checklists such as manuals from computer system vendors and publications from security organisations. Examples are BS7799 part 1 & 2 (1999), ISO/IEC TR 13335 Part 4 (1999), IT-Baseline Protection Manual (GISA 1997), and the NIST Handbook (1995). In these source materials, questions and checklists are generally listed by either functional areas such as input, processing and output, or asset types such as hardware, software and personnel. Therefore, we need to convert these generic checklists to specific questions tailored for risk analysis. The advantage of the checklist method is its simplicity in identifying major weaknesses.

The baseline approach is a simple way of performing risk analysis as it consists of (1) listing assets, (2) listing threats associated with each asset, (3) listing vulnerabilities associated with a pair of [asset, threat], (4) identifying existing controls for a triplet of [asset, threat, vulnerability], and (5) collecting all the information and assessing the measure of risk in a simple and pragmatic way (BS7799: Guide to Risk Assessment 1998). Once we have established a set of checklists that assess the vulnerability associated with each pair of asset and threat, the security review based on this set of checklists can be used as a baseline approach. A typical question in such a checklist may be 'given threat j on asset i, is there countermeasure k against threat j?' The main difference between our suggested approach and the BS7799 baseline approach is that we consider vulnerabilities and countermeasures simultaneously by using predefined checklist questions while BS7799 separates the identification of vulnerabilities and existing countermeasures. The suggested approach provides a much simpler evaluation by considering both vulnerabilities and corresponding countermeasures simultaneously. Although the checklist method does not provide the detailed insight found in a detailed risk analysis, it is still a useful method in that it gives us an overview of the system's security in a reasonably short time period. Also, it is the only applicable method where there is no risk analysis expertise or organisational resource such as budget and time to perform a detailed risk analysis.

One concern in the checklist method is how to manipulate the gathered answers so as to highlight areas that need management attention. Without a highlighting capability, the output of checklist-based risk analysis will be a lengthy list of answers to questions; such a list is of very limited use to management and prevents quick decisions for improving security. The most

common method for solving this problem is the use of a scoring method. In a simple scoring method, one may consider the following scheme:

Let N_i be the number of threats associated with asset i and N_{ij} be the number of vulnerability checkpoints (or questions) for threat j $(1 \le j \le N_i)$, which is associated with asset i. Assign the vulnerability score S_{ijk} $(1 \le k \le \max\{N_{ij} | 1 \le j \le N_i\})$ to each applicable vulnerability checkpoint. Assign $S_{ijk}=0$ where the checkpoint does not exist for a triplet (i,j,k). Then the measure of risk for asset i, denoted by R_i, can be calculated as follows:

$$R_i = \sum_j \sum_k N_i^{-1} N_{ij}^{-1} S_{ijk}$$

This measure represents the normalised sum of total vulnerability score associated with asset i. The normalisation is required as the number of vulnerability checkpoints and the number of threats varies with the assets and threats, respectively (each threat may have a different number of vulnerability checkpoints and each asset may have a different number of threats). The more advanced scoring method (i.e., the weighted average method) may appear in various forms. Examples include the following two equations.

If the weights (V_{ijk}) that are specific to each threat j are assigned to each vulnerability checkpoint, then R_i in the above example becomes:

$$R_i = N_i^{-1} \sum_j \sum_k V_{ijk} S_{ijk} \text{ where } \sum_k V_{ijk} = 1$$

If the weights (V_{ijk}) that are specific to each threat j are assigned to each vulnerability checkpoint, and the weights (T_{ij}) that are specific to each asset i are assigned to each threat j, then R_i in the above example becomes:

$$R_i = \sum_j \sum_k T_{ij} V_{ijk} S_{ijk} \text{ where } \sum_k V_{ijk} = 1, \ \sum_j T_{ij} = 1$$

3. UNCERTAINTY IN RISK ANALYSIS

Risk analysis must often rely on speculation, best guesses, incomplete data, and many unproven assumptions (The NIST Handbook 1995). Any risk measure based on the scoring method is sensitive to small changes in weights as well as changes in scores. Therefore, the uncertainty issues about scores and weights in the checklist method should be considered. According

to the NIST Handbook (1995), there are two primary sources of uncertainty: (1) a lack of confidence or precision in the risk analysis model or methodology, and (2) a lack of sufficient information to determine the exact value of the elements of the risk model. The correctness of the weight in the checklist method is related to the former while the correctness of the score is associated with the latter. Uncertainty is different from ambiguity; ambiguity is generally handled by the fuzzy set theory in risk analysis. According to Smets' (1991) contrast between imprecision (ambiguity) and uncertainty, imprecision covers cases where the value of a variable is given but not with the required precision, whereas uncertainty covers cases where an agent can construct a personal subjective opinion (belief) in a proposition that is not definitively established. Let us look at the following example: 'How much financial loss is incurred from the disclosure of specific data?' Assume that the analyst is sure that it would be a large loss although he cannot express the exact figure. In this case, the fuzzy theory can be applied. On the contrary, assume he thinks that it could be a large amount but is not sure about this because the actual loss might be much smaller than he expects. This situation represents the uncertainty in the analyst's opinion.

In this article, we will tackle the uncertainties associated with checklist method scores by adopting *plausibility* as a measure of risk, while avoiding the uncertainties associated with the weights by not considering them. In our checklist-based risk analysis, each asset is evaluated from a security preservation perspective by considering all the relevant controls. Non-existence or failure of any control could result in insecurity. This implies that all controls should be regarded as equally important *in terms of the security preservation* (this does not mean that we presume all controls are equally important when assessing the values of controls). With this strategy, we avoid the problem of weight assignment. Plausibility is a term used in belief functions (also known as Dempster-Shafer theory of evidence). Belief function is a general tool for representing someone's degree of belief in an uncertain situation. In this article, plausibility represents the potential insecurity after given evidence of security has been considered.

3.1 Evidential Network

In this article, the overall structure for measuring risk with uncertainty follows the structure of Srivastava's belief function formula (Srivastava and Shafer 1992, Srivastava and Mock 2000). He has developed a special network diagram to apply belief functions to various applications in the accounting domain such as the calculation of audit risk (Srivastava and Shafer 1992) and the WebTrust assurance service (Srivastava and Mock 2000). His model starts from building a network diagram called an evidential

network. In the evidential network, a rounded rectangle represents a variable and a proper rectangle represents evidence, which is connected to a variable that it directly supports. A circle with '&' implies that the variable on the left of the '&' is true if and only if the variables on the right of the '&' are true. Based on his model, we have applied the evidential network to a checklist-based risk analysis, as shown in figure 1. Each variable in an evidential network has a proposition. The proposition at the asset variable is 'asset *i* is secure' Similarly, the proposition at the threat variable is 'threat *j* will not be realised' and the proposition at the control variable is 'control *k* has been placed against threat *j*' It is assumed that the threat will not be realised if all corresponding controls function as intended. However, it does not mean that perfect security can be achieved. Our checklist method corresponds to the baseline approach, which is for baseline protection. The above propositions, 'asset *i* is secure' and 'threat will not be realised' imply that the risk will be reduced to an acceptable level as specified by the baseline protection. If an organisation feels that the checkpoints currently available for baseline protection are not sufficient to meet its baseline security, it may add some additional checkpoints at its own discretion. The proper rectangle 'control' represents the supporting evidence that the control, contributing to the prevention of the threat realisation, has been placed.

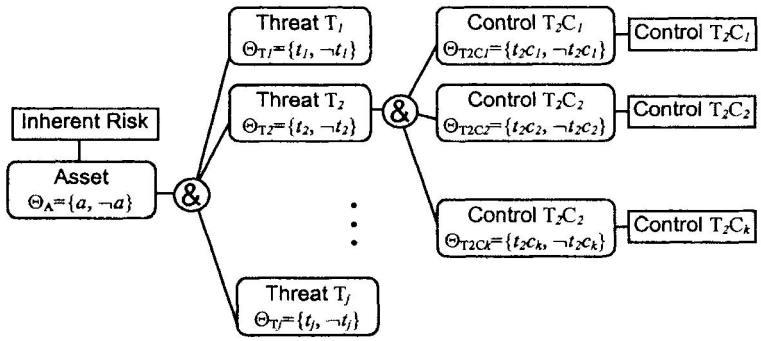

Figure 1. Evidential network for checklist-based risk analysis

This evidential network represents a framework for the checklist method mentioned earlier. The belief in the control corresponds to the score in the checklist method. The degree of belief is a number (not a probability) ranging from 0 to 1. High belief implies that there is strong evidential support for the given proposition. The degree of belief is determined by an analyst's feeling with respect to the given evidence. For example, the analyst feels that the control seems to be functioning as intended but he is not sure of this for some reason (e.g. he did not perform substantive tests or surveillance tests). He therefore decides to assign a medium level of belief to the

proposition that the control has been placed. At the same time, he has found a control malfunction such as the occasional bypass of the control. This gives him some degree of belief in the negation of the proposition. From these inputs to the 'control' rectangles, the plausibility of threat realisation and the plausibility of overall insecurity are calculated. The rectangle 'inherent risk' represents the potential insecurity resulting from factors beyond the scope of the security review. Examples of such factors are the lack of security awareness, lack of quality security management, potential security flaws and operational mistakes in new systems, and so on. These factors are not listed in the checklist but could cause the insecurity of an asset even if all the controls under review work properly. If the analyst feels that the inherent risk surrounding the asset is high, he will assign a high degree of belief to the negation of the proposition since risk is the opposite concept of security.

3.2 Basic Background for Belief Function Approach[1]

3.2.1 *m*-value

In evidence theory, traditional probabilities are replaced by the concept of evidential support. The contrast is between the chance that a hypothesis is true and the chance that the evidence proves that the hypothesis is true (Laskey and Cohen 1986). A frame of discernment, denoted by Θ, represents an exhaustive and mutually exclusive set of possible answers to a question. Instead of using probability, evidence theory uses the function m (called basic probability assignment) that assigns a number $m(\mathrm{B})$ to each subset B of Θ that satisfies:

a) $m(\emptyset)=0$
b) $m(\mathrm{B}) \geq 0$ for all $\mathrm{B} \subseteq \Theta$
c) $\sum\{m(\mathrm{B}) | \mathrm{B} \subseteq \Theta\}=1$

The way of assigning m-values in our model is by using a risk analyst's subjective judgment; this is the same as in Srivastava's model. The frame of discernment on the asset variable (Θ_{A}) has two elements, a and its negation ($\neg a$). Therefore there exist three m-values such as $m_{\mathrm{A}}(\{a\})$, $m_{\mathrm{A}}(\{\neg a\})$ and $m_{\mathrm{A}}(\{a,\neg a\})$. For simplicity, we will write $m_{\mathrm{A}}(a)$ and $m_{\mathrm{A}}(\neg a)$ instead of $m_{\mathrm{A}}(\{a\})$ and $m_{\mathrm{A}}(\{\neg a\})$. The subscript represents the name of variable to which evidence is applied ('A' stands for the asset variable in this case). The

[1] A major part of this section is based on Srivastava and Shafer (1992).

element 'a' represents, for example, the proposition that 'asset i is secure' and the element '$\neg a$' represents the proposition that 'asset i is NOT secure'. The way of assigning m-values is as follows. Assume that an analyst feels that the given evidence supports the proposition a with a medium level (say, 0.6) of support and he feels that there is no evidence supporting $\neg a$. Thus, he assigns $m_A(a)=0.6$ and $m_A(\neg a)=0$. $m_A(\{a,\neg a\})=1-m_A(a)-m_A(\neg a)$ represents the ignorance (the amount committed to neither a nor $\neg a$).

3.2.2 Belief and Plausibility

The total belief in a subset B of a frame Θ is defined as $Bel(B)=\sum\{m(X)|\ X\subseteq B\}$ for all $B\subseteq\Theta$, and the plausibility of B is defined as $pl(B)=\sum\{m(X)|\ B\cap X\neq\emptyset\}=1-Bel(\neg B)$. The value $Bel(B)$ summarises all our reasons for believing B under the given evidence, and the value $pl(B)$ represents how much we should believe B if all currently unknown facts (i.e., underlying ignorance) were to support B. The difference is that $Bel(B)$ quantifies the total amount of justified supports given to B, while $pl(B)$ quantifies the maximum amount of potential supports that could be given to B. Similarly, it can be shown that $pl(\neg B)=1-Bel(B)$, which represents the degree to which $\neg B$ is plausible. In the evidential network in figure 1, every variable has only two propositions and thus the frame on each variable has only two elements. For example, $Bel_X(x)=m_X(x)$ and $Bel_X(\neg x)=m_X(\neg x)$ for a frame $\Theta_X=\{x,\neg x\}$. The plausibility of the negation of the statement has an important interpretation as it represents the measure of risk in our risk analysis model; how plausible is the occurrence of insecurity.

3.2.3 Dempster's Rule of Combination

If $m_1(B)$ and $m_2(B)$ are two m-values on the same frame Θ induced by two independent evidential resources, then the combined m-value is calculated according to Dempster's rule (Shafer 1976) which is $m(B)=m_1\oplus m_2(B)=k^{-1}\sum\{m_1(X_1)m_2(X_2)|\ X_1\cap X_2=B\}$, where $k=1-\sum\{m_1(X_1)m_2(X_2)|\ X_1\cap X_2=\emptyset\}$, a normalization constant. Normalization is required to satisfy the axiom that the sum of m-values on a frame equals 1 where a conflict $(\sum\{m_1(X_1)m_2(X_2)|\ X_1\cap X_2=\emptyset\}>0)$ exists. Dempster's rule cannot be used when $k=0$, in which case the two items are not combinable.

3.2.4 Belief Propagation: Forward Direction

In figure 1, the asset is linked with several threats and each threat is linked with several relevant controls. To obtain m-values for the asset variable, we need to calculate the m-values propagated from the input nodes

i.e., controls. The evidential network in figure 1 is an AND-tree, which means that the proposition at the asset variable is true if and only if all the propositions on threat variables are true. Likewise, the proposition at each threat variable is true if and only if all the propositions at the controls associated with the threat are true. First, let us consider the propagation of *m*-values (from all the controls associated with threat *x*) to threat *x*. Assume that there are *N* controls associated with threat *x*. Let $m_{\mathrm{T}x\mathrm{C}y}(t_x c_y)$, $m_{\mathrm{T}x\mathrm{C}y}(\neg t_x c_y)$ and $m_{\mathrm{T}x\mathrm{C}y}(\{t_x c_y, \neg t_x c_y\})$ be the *m*-values at control variable T*x*C*y*, obtained from the proper rectangle 'Control T*x*C*y*'. These *m*-values are based on an analyst's opinion on the existence/status of control *i*. The propagated *m*-values at threat *x*, denoted by $m_{\mathrm{T}x \leftarrow all\ \mathrm{C}'s\ of\ \mathrm{T}x}(\theta_{\mathrm{T}x})$ (where $\theta_{\mathrm{T}x} \subseteq \Theta_{\mathrm{T}x}$ and $\theta_{\mathrm{T}x} \neq \emptyset$), are calculated as follows:

1. $m_{\mathrm{T}x \leftarrow all\ \mathrm{C}'s\ of\ \mathrm{T}x}(t_x) = \prod_{i=1}^{\mathrm{N}} m_{\mathrm{T}x\mathrm{C}i}(t_x c_i)$
2. $m_{\mathrm{T}x \leftarrow all\ \mathrm{C}'s\ of\ \mathrm{T}x}(\neg t_x) = 1 - \prod_{i=1}^{\mathrm{N}} [1 - m_{\mathrm{T}x\mathrm{C}i}(\neg t_x c_i)]$
3. $m_{\mathrm{T}x \leftarrow all\ \mathrm{C}'s\ of\ \mathrm{T}x}(\{t_x, \neg t_x\}) = 1 - m_{\mathrm{T}x \leftarrow all\ \mathrm{C}'s\ of\ \mathrm{T}x}(t_x) - m_{\mathrm{T}x \leftarrow all\ \mathrm{C}'s\ of\ \mathrm{T}x}(\neg t_x)$

The propagation from the threat variables to the asset variable is similar to the above. Let *P* be the number of threats. The propagated *m*-values at the asset variable, denoted by $m_{\mathrm{A} \leftarrow all\ \mathrm{T}'s}(\theta_{\mathrm{A}})$ (where $\theta_{\mathrm{A}} \subseteq \Theta_{\mathrm{A}}$ and $\theta_{\mathrm{A}} \neq \emptyset$), are as follows:

4. $m_{\mathrm{A} \leftarrow all\ \mathrm{T}'s}(a) = \prod_{i=1}^{\mathrm{P}} m_{\mathrm{T}i \leftarrow all\ \mathrm{C}'s\ of\ \mathrm{T}i}(t_i)$
5. $m_{\mathrm{A} \leftarrow all\ \mathrm{T}'s}(\neg a) = 1 - \prod_{i=1}^{\mathrm{P}} [1 - m_{\mathrm{T}i \leftarrow all\ \mathrm{C}'s\ of\ \mathrm{T}i}(\neg t_i)]$
6. $m_{\mathrm{A} \leftarrow all\ \mathrm{T}'s}(\{a, \neg a\}) = 1 - m_{\mathrm{A} \leftarrow all\ \mathrm{T}'s}(a) - m_{\mathrm{A} \leftarrow all\ \mathrm{T}'s}(\neg a)$

3.2.5 Measure of Risk

From equations 1, 2 and 3, we can obtain the *m*-values propagated from the controls to the threats. These *m*-values are also propagated to the asset variable and the results of this propagation are obtained from equations 4, 5 and 6. We apply Dempster's rule to combine these propagated *m*-values with the *m*-values (denoted by $m_{\mathrm{A}}(\theta_{\mathrm{A}})$, where $\theta_{\mathrm{A}} \subseteq \Theta_{\mathrm{A}}$ and $\theta_{\mathrm{A}} \neq \emptyset$) obtained from the proper rectangle 'inherent risk'. This yields the following *m*-values for the asset variable:

7. $m^t_{\mathrm{A}}(a) = m_{\mathrm{A}} \oplus m_{\mathrm{A} \leftarrow all\ \mathrm{T}'s}(a)$
8. $m^t_{\mathrm{A}}(a) = m_{\mathrm{A}} \oplus m_{\mathrm{A} \leftarrow all\ \mathrm{T}'s}(\neg a)$
9. $m^t_{\mathrm{A}}(\{a, \neg a\}) = 1 - m^t_{\mathrm{A}}(a) - m^t_{\mathrm{A}}(\neg a)$

The superscript '*t*' indicates that these *m*-values are the resulting (total) *m*-values after all evidence in the AND-tree has been considered. As

mentioned above, the plausibility of the negation of the proposition at the asset variable, $pl_A(\neg a)=1-Bel_A(a)$, is the measure of risk in our model, which represents the degree to which insecurity is plausible. The measure of risk, $pl_A(\neg a)$ is $1-m^t{}_A(a)$ as $Bel_A(a)=m^t_A(a)$.

3.2.6 Belief Propagation: Backward Direction

The belief (m-values) is also propagated in the opposite direction (from asset to each threat, and from each threat to relevant controls) as well as the propagation mentioned above. We need to consider this propagation to obtain the resulting m-values for threats and controls. It means that the m-values obtained from the inherent risk node should be propagated to each threat and to each control since this inherent risk affects the security status at threat and control levels. We need to consider this propagation when we want to obtain the marginal risk measures such as the plausibility of the threat realisation and the plausibility of the control malfunction/failure. These measures are not required for the calculation of the measure of risk at asset level. However, it provides useful information to management (e.g. which threat is likely to be realised and which control is likely not to be guaranteed). The m-values propagated from the asset to threat x, denoted by $m_{Tx\leftarrow A\ \&\ all\ other\ T's}(\theta_{Tx})$ (where $\theta_{Tx}\subseteq\Theta_{Tx}$ and $\theta_{Tx}\neq\emptyset$), are as follows:

10. $m_{Tx\leftarrow A\ \&\ all\ other\ T's}(t_x)=k_x^{-1}m_A(a)\prod^P_{i=1,i\neq x}[1-m_{Ti\leftarrow all\ C's\ of\ Ti}(\neg t_i)]$
11. $m_{Tx\leftarrow A\ \&\ all\ other\ T's}(\neg t_x)=k_x^{-1}m_A(\neg a)\prod^P_{i=1,i\neq x}m_{Ti\leftarrow all\ C's\ of\ Ti}(t_i)$
12. $m_{Tx\leftarrow A\ \&\ all\ other\ T's}(\{t_x,\neg t_x\})=1-m_{Tx\leftarrow A\ \&\ all\ other\ T's}(t_x)-m_{Tx\leftarrow A\ \&\ all\ other\ T's}(\neg t_x)$

where k_x is the normalization constant, which is given by $k_x=1-m_A(a)\cdot C_x$, where C_x is given by $C_x=1-\prod^P_{i=1,i\neq x}[1-m_{Ti\leftarrow all\ C's\ of\ Ti}(\neg t_i)]$

Then, the resulting m-values at threat x are as follows:

13. $m^t{}_{Tx}(t_x)=m_{Tx\leftarrow all\ C's\ of\ Tx}\oplus m_{Tx\leftarrow A\ \&\ all\ other\ T's}(t_x)$
14. $m^t{}_{Tx}(\neg t_x)=m_{Tx\leftarrow all\ C's\ of\ Tx}\oplus m_{Tx\leftarrow A\ \&\ all\ other\ T's}(\neg t_x)$
15. $m^t{}_{Tx}(\{t_x,\neg t_x\})=1-m^t{}_{Tx}(t_x)-m^t{}_{Tx}(\neg t_x)$

Similarly, the m-values propagated from threat x to control y (that is associated with threat x), denoted by $m_{TxCy\leftarrow Tx\ \&\ all\ other\ C's\ of\ Tx}(\theta_{TxCy})$ where $\theta_{TxCy}\subseteq\Theta_{TxCy}$ and $\theta_{TxCy}\neq\emptyset$), are as follows:

16. $m_{TxCy\leftarrow Tx\ \&\ all\ other\ C's\ of\ Tx}(t_xc_y)$
$=k_{xy}^{-1}m_{Tx\leftarrow A\ \&\ all\ other\ T's}(t_x)\prod^N_{i=1,i\neq y}[1-m_{TxCi}(\neg t_xc_i)]$
17. $m_{TxCy\leftarrow Tx\ \&\ all\ other\ C's\ of\ Tx}(\neg t_xc_y)$

$$=k_{xy}^{-1} m_{\mathrm{Tx}\leftarrow \mathrm{A}\ \&\ all\ other\ \mathrm{T}'s}(\neg t_x)\prod_{i=1,i\neq y}^{\mathrm{N}} m_{\mathrm{Tx}\mathrm{C}i}(t_x c_i)$$

18. $m_{\mathrm{Tx}\mathrm{C}y\leftarrow \mathrm{Tx}\ \&\ all\ other\ \mathrm{C}'s\ of\ \mathrm{Tx}}(\{t_x c_y, \neg t_x c_y\})$
$=1-m_{\mathrm{Tx}\mathrm{C}y\leftarrow \mathrm{Tx}\ \&\ all\ other\ \mathrm{C}'s\ of\ \mathrm{Tx}}(t_x c_y)-m_{\mathrm{Tx}\mathrm{C}y\leftarrow \mathrm{Tx}\ \&\ all\ other\ \mathrm{C}'s\ of\ \mathrm{Tx}}(\neg t_x c_y)$

where k_{xy} the normalization constant, which is given by $k_{xy}=1-m_{\mathrm{Tx}\leftarrow \mathrm{A}\ \&\ all\ other\ \mathrm{T}'s}(t_x)\cdot C_{xy}$, where C_{xy} is given by $C_{xy}=1-\prod_{i=1,i\neq y}^{N}[1-m_{\mathrm{Tx}\mathrm{C}i}(\neg t_x c_i)]$

Then, the resulting m-values at control y that is associated with threat x are as follows:

19. $m^{t}_{\mathrm{Tx}\mathrm{C}y}(t_x c_y)= m_{\mathrm{Tx}\mathrm{C}y}\oplus m_{\mathrm{Tx}\mathrm{C}y\leftarrow \mathrm{Tx}\ \&\ all\ other\ \mathrm{C}'s\ of\ \mathrm{Tx}}(t_x c_y)$
20. $m^{t}_{\mathrm{Tx}\mathrm{C}y}(\neg t_x c_y)= m_{\mathrm{Tx}\mathrm{C}y}\oplus m_{\mathrm{Tx}\mathrm{C}y\leftarrow \mathrm{Tx}\ \&\ all\ other\ \mathrm{C}'s\ of\ \mathrm{Tx}}(\neg t_x c_y)$
21. $m^{t}_{\mathrm{Tx}\mathrm{C}y}(\{t_x c_y, \neg\ t_x c_y\})=1-m^{t}_{\mathrm{Tx}\mathrm{C}y}(t_x c_y)-m^{t}_{\mathrm{Tx}\mathrm{C}y}(\neg t_x c_y)$

4. EXAMPLES

4.1 Security of Data Asset

In this section, we provide a numerical example to show how our risk analysis method can be used. Our example is the security review of the controls for securing a specific data asset. The review of security preservation on a data asset requires an extensive review process because the security of data asset could be affected by many sources of insecurity. For example, an attacker could get access to the data asset by exploiting security flaws in the operating system. However, the full simultaneous examination of all the possible security holes that could affect the security of the data asset is not efficient in the checklist method since it generates a very lengthy list of questions for each asset. Therefore, some assumptions and omissions are required to achieve quick and efficient reviews. The main purpose of the baseline approach is to ensure that all identified assets are protected to a baseline level. Once we assume that all the major vulnerabilities are identified by relevant baseline security reviews, we can narrow down the focus of our review. The review of the data asset in our example assumes that other vulnerabilities have been examined in other review categories. For example, unavailability of the data asset has been excluded as it is assumed that this issue is to be examined by the reviews for unavailability of server, client, network component and backup media. For simplicity, our example includes only two threats with three controls per threat. The overall structure of the example is shown in figure 2.

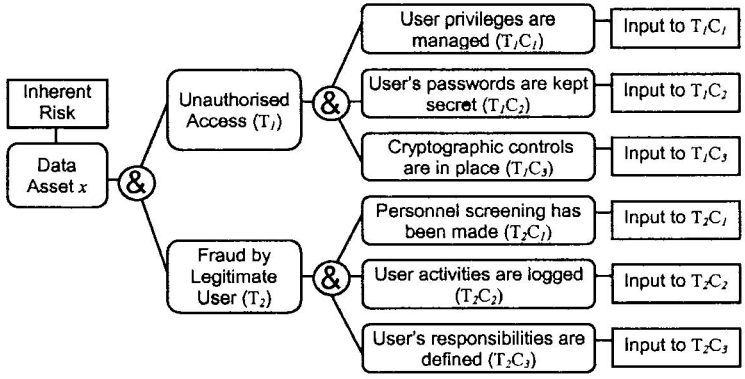

Figure 2. The example network for data asset checklist

Assume that a risk analyst has reviewed the client application for the data asset x against relevant controls, and provided the m-values for each control as shown in table 1. The way of assigning m-values can be illustrated with the following example. Consider that the analyst has found that well-defined access control lists exist in the organisation but he is not sure whether they preserve the principle of least privilege. Therefore, he assigned 0.6 as support for the proposition that user privileges are managed. At the same time, he assigned 0 as support for the negation of the proposition since he did not find any evidence of bad user privilege management practices. These values are shown in the first column (T*1C1*) in table 1.

Table 1. Input Values for Example

	T*1C1*	T*1C2*	T*1C3*	T2C*1*	T2C*2*	T2C*3*	Inherent Risk
support	.6	. 5	.7	.9	.7	.7	.7
Neg. Support	.0	.3	.2	.0	.2	.0	.0

As for the input values for inherent risk, the analyst feels that there is top management commitment to security and a mature security culture in the organisation; these are positive factors for the proposition that the data asset is protected from the viewpoint of user's behaviour. He thus assigned 0.7 support for the proposition that the data asset x is protected. Excluding the last column, the values in table 1 represent the m-values for $m_{\mathrm{T}i\mathrm{C}j}(t_i c_j)$ and $m_{\mathrm{T}i\mathrm{C}j}(\neg t_i c_j)$ (i=1,2 and j =1,2,3). The values in the last column represent the m-values for $m_{\mathrm{A}}(a)$ and $m_{\mathrm{A}}(\neg a)$. Based on these m-values provided by the analyst, we can calculate all the m-values required for obtaining the measure of risk; how plausible the insecurity of the data asset x is. The calculation results are shown in table 2.

Table 2. Calculation Procedures for Measure of Risk

$m_{T1\leftarrow \text{all C's of } T1}(t_1)= 0.210$, $m_{T1\leftarrow \text{all C's of } T1}(\neg t_1)= 0.440$
$m_{T2\leftarrow \text{all C's of } T2}(t_2)= 0.441$, $m_{T2\leftarrow \text{all C's of } T2}(\neg t_2)= 0.200$
$m_{A\leftarrow \text{all T's}}(a)=0.093$, $m_{A\leftarrow \text{all T's}}(\neg a)=0.552$
$m'_A(a)=0.556$, $m'_A(\neg a)=0.270$ $\therefore$ $pl_A(\neg a)=0.444$
$m_{T1\leftarrow A \text{ \& all other T's}}(t_1)=0.651$, $m_{T1\leftarrow A \text{ \& all other T's}}(\neg t_1)=0.000$
$m'_{T1}(t_1)=0.614$, $m'_{T1}(\neg t_1)=0.215$ $\therefore$ $pl_{T1}(\neg t_1)=0.386$
$m_{T2\leftarrow A \text{ \& all other T's}}(t_2)=0.566$, $m_{T2\leftarrow A \text{ \& all other T's}}(\neg t_2)=0.000$
$m'_{T2}(t_2)=0.727$, $m'_{T2}(\neg t_2)=0.098$ $\therefore$ $pl_{T2}(\neg t_2)=0.273$
$m_{T1C1\leftarrow T1 \text{ \& all other C's of } T1}(t_1c_1)=0.511$, $m_{T1C1\leftarrow T1 \text{ \& all other C's of } T1}(\neg t_1c_1)=0.000$
$m_{T1C2\leftarrow T1 \text{ \& all other C's of } T1}(t_1c_2)=0.599$, $m_{T1C2\leftarrow T1 \text{ \& all other C's of } T1}(\neg t_1c_2)=0.000$
$m_{T1C3\leftarrow T1 \text{ \& all other C's of } T1}(t_1c_3)=0.566$, $m_{T1C3\leftarrow T1 \text{ \& all other C's of } T1}(\neg t_1c_3)=0.000$
$m'_{T1C1}(t_1c_1)=0.804$, $m'_{T1C1}(\neg t_1c_1)=0.000$ $\therefore$ $pl_{T1C1}(\neg t_1c_1)=0.196$
$m'_{T1C2}(t_1c_2)=0.756$, $m'_{T1C2}(\neg t_1c_2)=0.147$ $\therefore$ $pl_{T1C2}(\neg t_1c_2)=0.244$
$m'_{T1C3}(t_1c_3)=0.853$, $m'_{T1C3}(\neg t_1c_3)=0.098$ $\therefore$ $pl_{T1C3}(\neg t_1c_3)=0.147$
$m_{T2C1\leftarrow T2 \text{ \& all other C's of } T2}(t_2c_1)=0.511$, $m_{T2C1\leftarrow T2 \text{ \& all other C's of } T2}(\neg t_2c_1)=0.000$
$m_{T2C2\leftarrow T2 \text{ \& all other C's of } T2}(t_2c_2)=0.566$, $m_{T2C2\leftarrow T2 \text{ \& all other C's of } T2}(\neg t_2c_2)=0.000$
$m_{T2C3\leftarrow T2 \text{ \& all other C's of } T2}(t_2c_3)=0.511$, $m_{T2C3\leftarrow T2 \text{ \& all other C's of } T2}(\neg t_2c_3)=0.000$
$m'_{T2C1}(t_2c_1)=0.951$, $m'_{T2C1}(\neg t_2c_1)=0.000$ $\therefore$ $pl_{T2C1}(\neg t_2c_1)=0.049$
$m'_{T2C2}(t_2c_2)=0.853$, $m'_{T2C2}(\neg t_2c_2)=0.098$ $\therefore$ $pl_{T2C2}(\neg t_2c_2)=0.147$
$m'_{T2C3}(t_2c_3)=0.853$, $m'_{T2C3}(\neg t_2c_3)=0.000$ $\therefore$ $pl_{T2C3}(\neg t_2c_3)=0.147$

The measure of risk in this example is 0.444. Table 2 also shows the final m-values at threat and control variables after belief propagation in the backward direction. The plausibility of the realisation of unauthorised access is 0.386 whereas the plausibility of the realisation of fraud attempt is 0.273. From these results, we can conclude that unauthorised access is more likely to occur than a fraud attempt. As our evidential network diagram indicates, the measure of risk is sensitive to the changes of m-values arising from the inherent risk node. If the analyst is competent and has enough knowledge of the organisation's information system, consideration of the inherent risk would provide a more precise reflection of organisational security issues. Otherwise, it may produce the wrong result. Therefore, if he cannot provide any opinion/answer to the question X in the checklist, he may leave the question unanswered. In this case, $m_X(x)=m_X(\neg x)=0$ will be assigned, which means $m_X(\{x,\neg x\})=1$. This is equally applicable to the inherent risk node. Another concern in using evidential reasoning is that this approach requires more inputs than conventional checklist methods. If we assume that the evidence is affirmative, i.e., the evidence supports a proposition and does not support its negation, the number of inputs required may be reduced to the levels found in the conventional checklist method. Obtaining risk measures by evidential reasoning includes a tedious calculation process. Therefore, a computerised facility for belief calculation should be embedded in the checklist-based analysis tool.

4.2 BS7799 Self-Assessment by Evidential Reasoning

The evidential network specified in this article can also be used for self-assessment of BS7799 compliance without any major modification of the network structure. Self-assessment refers to the assessment performed by an organisation (internally) to check whether it is ready for a formal assessment against the Accredited Certification Scheme for BS7799 Part 2. BS7799 Part 2 (1999) provides a summarised list of controls and control objectives in ten assessment categories so that the controls specified by BS7799 can be examined more clearly.

To apply BS7799 self-assessment, the asset variable in figure 1 should be replaced by the variable 'assessment category', the threat variable should be replaced by the variable 'control objective', and the control variable should be replaced by the variable 'control procedure' that ensures the relevant control objective. For example, BS7799 Part 2 specifies three control objectives for physical and environmental security (Assessment Category *5*). One is to prevent unauthorised access, damage and interference to business premises and information (Control Objective *5.1*). Another is to prevent loss, damage or compromise of assets and interruption to business activities (Control Objective *5.2*). The third is to prevent compromise or theft of information and information processing facilities (Control Objective *5.3*). Each control objective is associated with several relevant controls. For example, there are two controls for the Control Objective *5.3*:

- Clear desk and clear screen policy: Organisations shall have and implement a clear desk and a clear screen policy in order to reduce the risks of unauthorised access, loss, and damage to information (Control *5.3.1*)
- Removal of property: Equipment, information or software belonging to the organisation shall not be removed without authorisation (Control *5.3.2*).

The inherent risk node in figure 1 can also be used in the BS7799 self-assessment structure since the concepts are still valid. The proposition at assessment category x is that category x satisfies the certification requirements. The proposition at the control objective $x.y$ is that the control objective y belonging to the category x meets the requirements for the certification. The proposition at the control $x.y.z$ is that the control procedure z belonging to the control objective $x.y$ satisfies the control requirement for the certification. The guidelines for assessing each control against BS7799 certification are provided in 'BS7799: Preparing for BS7799 certification (1999)'.

5. CONCLUSION

In this article, we have examined the applicability of evidential reasoning in the risk analysis domain. Most risk analysis methods force the analyst to provide subjective opinions in the course of the evaluation. Therefore, the belief function approach can be an alternative to these conventional risk analysis methods. Because evidential reasoning using AND-trees originated from accounting domains such as audit risk assessment, it could be modified to accommodate checklist-based risk analysis without much difficulty. Belief functions can be used instead of the conventional approach based on probability theory. The advantage of using belief functions is their ability to deal with uncertainty. In probability theory, the sum of the probability of event occurrence and the probability of its complement should be 1. However, this restriction is relaxed in evidence theory by introducing the concept of ignorance.

The major drawback of quantitative risk analysis methodologies is the difficulty in estimating probabilities since quantitative methods rely heavily on the accuracy of the estimates. Although evidence theory does not provide a clear answer to this problem (since it still requires *m*-values, which are regarded as meta probabilities over a probability that is to be estimated), it may provide, to some extent, the relaxation in accuracy needed when expressing uncertainty. The problem of qualitative risk analysis is that the risk is often based on subjective judgment. Although detailed guidelines for assigning qualitative values are provided in many qualitative methods, the answers provided by analysts still rely on their own subjective opinions. This problem can also be handled by evidence theory. In summary, evidence theory offers a new way of thinking about risk analysis.

REFERENCES

BS7799: Guide to BS7799 Risk Assessment and Risk Management, British Standard Institution, 1998

BS7799: Part 1: Code of Practice for Information Security Management, British Standard Institution, 1999

BS7799: Part 2: Specification for Information Security Management Systems, British Standard Institution, 1999

BS7799: Preparing for BS7799 Certification, British Standard Institution, 1999

CCTA, An Overview of CRAMM, CCTA IT Security and Privacy Group, UK, 1990

Ciechanowicz, Z., Risk Analysis Requirements, Conflicts and Problems, Computers & Security, 1997, Vol. 16, No. 3, pp. 223-232

Erwin, D., The Thirty-Minute Risk Analysis, Information Systems Security, 1994, Vo1.3, No. 3, pp. 37-44

GISA (German Information Security Agency), IT-Baseline Protection Manual, Bundesamt für Sicherheit in der Informationstechnik, 1997

ISO/IEC TR 13335-1, Guideline for Management of IT Security-Part1: Concepts and Models for IT security, 1996

ISO/IEC TR 13335-2, Guideline for Management of IT Security-Part2: Managing and Planning of IT Security, 1997

ISO/IEC TR 13335-3, Guideline for Management of IT Security-Part3: Techniques for the Management of IT Security, Working Draft, 1997

ISO/IEC TR 13335-4, Guideline for Management of IT Security-Part4: Selection of Safeguards, 1999

Laskey, K.B. and Cohen, M.S., Applications of the Dempster-Shafer Theory of Evidence, Proceedings of the 1986 Winter Simulation Conference, December 8-10, 1986, Washington, DC, pp. 440-444

NIST, An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, 1995

Pfleeger, C.P., Security in Computing, 2nd Edition, Prentice-Hall, NJ, 1997

Rainer, R.K., Snyder, C.A. and Carr, H.H., Risk Analysis for Information Technology, Journal of Management Information Systems, 1991, Vol. 8, No. 1, pp. 129-147

Shafer, G.R., A Mathematical Theory of Evidence, Princeton University Press, NJ, 1976

Smets, P., Varieties of Ignorance and the Need for Well-Founded Theories, Information Sciences, 1991, Vol. 57-58, pp. 135-144.

Srivastava, R.P. and Mock, T.J., Evidential Reasoning for WebTrust Assurance Services, Journal of Management Information Systems, 1999-2000; Vol. 16, No. 3, pp. 11-32

Srivastava, R.P. and Shafer, G.R., Belief-Function Formulas for Audit Risk, The Accounting Review, 1992, Vol. 67, No. 2, pp. 249-283