Journal Emerging Technologies in Accounting, Vol. 5, No. 1, 2008, pp. 189-219

Risk and Reliability Formulas for Systems Security Under Dempster-Shafer Theory of Belief Functions

Rajendra P. Srivastava
Ernst & Young Distinguished Professor and Director
Ernst and Young Center for Auditing Research and Advanced Technology
1300 Sunnyside Avenue
The University of Kansas
Lawrence, KS 66045
Email: rsrivastava@ku.edu

Chan Li
Assistant Professor
Katz Graduate School of Business
University of Pittsburgh
Pittsburgh, PA 15260
Email: chanli@katz.pitt.edu

July 2008

Acknowledgements: The authors would like to express our thanks for valuable comments received on an earlier version of this paper, provided by the participants of The University of Kansas Accounting and Information Systems Workshop, Lawrence, Kansas; the participants of the Annual Meeting of the American Accounting Association, San Francisco, August 2005; and the participants of the 2005 Midyear AIS Meeting, New Orleans. In particular, the authors would like to thank Carol Brown for the insightful comments on an earlier version of the paper.

Risk and Reliability Formulas for Systems Security Under Dempster-Shafer Theory of Belief Functions

ABSTRACT

This paper develops comprehensive formulas for assessing the risk and reliability of "Systems Security" under Dempster-Shafer theory of belief functions using the Trust Services framework as proposed by American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA). In addition, we discuss how these formulas can be used for planning and evaluation of "Systems Security" risk under the SysTrust services. The analytical formulas are derived for a tree-structured evidential diagram which is constructed by converting the exact network-structured evidential diagram. The use of an analytical formula eliminates the computational complexities of propagating beliefs in a network and allows the assurance provider to use simple spreadsheet to combine evidence. We provide theoretical justification and perform sensitivity analyses to show that the analytical formula based on a tree type evidential diagram is a good approximation of the exact network model under realistic situations. However, as shown theoretically and also through the sensitivity analysis that the analytical formula provides significantly different results when input beliefs are significantly negative. It should be noted that the analytical formula based on the tree model provides a more conservative assessment of information systems risk than the exact network model.

Key Words: Systems Reliability, Systems Security Risk, Belief Functions, Dempster-Shafer Theory

Risk and Reliability Formulas for Systems Security Under Dempster-Shafer Theory of Belief Functions

INTRODUCTION

The purpose of this paper is to develop comprehensive analytical formulas for assessing the risk and reliability of "Systems Security" under Dempster-Shafer (hereafter DS, Shafer 1976) theory of belief functions. "Systems security" is one of the five principles of SysTrust services being performed by the AICPA/CICA (2003). In addition, we discuss how these formulas can be used for planning and evaluation of systems security risks when providing the assurance under the SysTrust services. To date, there is no analytical formula for planning and evaluation of systems security risk as it is available for financial statement audit (e.g. SAS 47, Srivastava and Shafer 1992). Under the SysTrust services, the principle "Systems Security" implies that the system is protected against unauthorized access (both physical and logical). We use the "Systems Security" principle as an illustration for deriving the formulas for its risk and reliability (definitions of risk and reliability are given in the next section). The steps involved in deriving the risk and reliability formulas for the other four principles, Availability, Processing Integrity, Online Privacy, and Confidentiality, are identical to the present case and thus we do not derive the formulas for these principles.

The analytical formulas developed in this paper are comprehensive in the sense that they include all types of evidence[1], positive, negative, or mixed. In contrast, Srivastava and Shafer (1992) in deriving the audit risk formula, assumed only positive (affirmative) items of evidence. This was primarily because the general theoretical work was not available for propagating beliefs

[1] Positive evidence means that the evidence only supports the assertion and has no information about its negation. Negative evidence means that the evidence supports the negation of the assertion and has no information in support of the assertion. Mixed evidence means that the evidence partly supports the assertion and partly negates the assertion.

in an evidential diagram with a tree type structure with multiple items of evidence that pertain to each variable in a tree (Srivastava, Shenoy and Shafer 1995, Srivastava 2005).

Basically, in any assurance process, the assurance provider collects, evaluates and aggregates items of evidence pertaining to the assertion or its sub-assertions to determine whether the assertion is met or not met to provide an appropriate opinion (see, e.g., Srivastava and Shafer 1992, Srivastava 1995, Srivastava, Dutta, and Johns 1996). In general, there are three important issues related to the development of analytical formulas for the risk and reliability assessment. First, there are inherent uncertainties associated with the items of evidence, i.e., none of the items of evidence collected in the assurance process provide absolute assurance that the assertion or the sub-assertion is either met or not met. We get only partial support in favor of the assertion or sub-assertion that it is met or not met. There are several frameworks, such as probability theory, fuzzy logic, and DS theory of belief functions that could be used to model uncertainties in the evidence. We use DS theory to model uncertainties involved in the evidence because it provides a flexible and adaptable way to combine evidence from a variety of sources (see, e.g., Akresh, Loebbecke, and Scott 1988, Gordon and Shortliffe 1990). In addition, there is empirical evidence both in auditing (Harrison et al. 2002) and in psychology (Curly and Golden 1994) that decision makers' judgments about uncertainties can be mapped better under DS theory than probability theory. Harrison et al. (2002) empirically found that 80 percent of auditors' (seniors and managers) judgments of uncertainties could be modeled only using DS theory. Similarly, Curley and Golden (1994) found that business students serving as jurors to analyze a case with four possible suspects and up to four pieces of evidence pertaining to the suspects did assign probability mass to subsets that were logically consistent with DS theory.

The second issue deals with the structure of evidence, i.e., how various items of evidence relate to different assertions and sub-assertions in the problem domain of interest (see, e.g., Sun, Srivastava, and Mock 2006). To deal with the second issue we develop an evidential diagram which consists of assertions and sub-assertions pertaining to the "Systems Security" principle and the corresponding items of evidence as described by AICPA/CICA (1993).

The third issue deals with the nature of evidence, i.e., whether the item of evidence is positive, negative or mixed. As mentioned earlier, positive item of evidence means that the evidence supports the assertion but has no information about its negation. A negative piece of evidence means that it supports the negation of the assertion or sub-assertion but has no information in its support, whereas a mixed item of evidence implies that the evidence partly supports the assertion and partly negates it. The DS theory used in the present paper models all such items of evidence appropriately while probability theory can model only mixed items of evidence. For example, if one assumes under probability theory that an assertion is true with 0.7 level of support then by definition 0.3 level of support is assigned to the negation of the assertion whether the evidence has any information about its negation or not. However, under DS theory, such an item of evidence can be represented as 0.7 level of support for the assertion being true, zero level of support for its negation, and 0.3 level of support unassigned representing the ignorance. As described later in the paper, we use the evidential diagram approach under DS theory to propagate beliefs from various levels of the diagram to derive the analytical formulas.

It is important to point out that companies are now relying heavily on information systems. Enterprise Resource Planning (ERP) systems connect all of a company's functional areas. System failure could bring disastrous consequences to a company's business, its image, and its strategic partnership with a third party. For example, problems of the warehouse automation systems of FoxMeyer Drug Company led the company to file for bankruptcy (Scott 1999). Great North Foods, Inc. found itself in big trouble when its supplier, Hershey Foods Corp., failed to deliver 9,000 kg of candy right before Halloween because Hershey's computer system was down (Boritz et al. 2000). Worldwide IT spending will surpass $3.3 trillion in 2008, a 5.5 percent increase from 2007 (Brodkin 2007). As a result, the risk of systems failure is becoming even more consequential. The formulas developed here provide a structured approach to assessing the risk and reliability of a system.

Section 404 of the landmark Sarbanes-Oxley Act (SOX) of 2002 requires public companies to report on the effectiveness of internal control systems. It requires auditors to attest management's report, as well as provide their own reports on the effectiveness of the internal control systems. In light of the fact that most companies' business transactions are routinely electronic, information systems have become an integral part of companies' internal control systems. The Public Company Accounting Oversight Board (PCAOB) specifically states that information systems controls should be considered as company-level controls, given the extensive and pervasive usage of information systems in companies' daily business processes and transactions (PCAOB, 2004). Recent studies suggest that company-level control problems are more severe than account- or transaction-level control problems (e.g., Doyle et al. 2007, and Ettredge et al. 2007). Because information systems play an important role not only in companies' daily business, but also in companies' overall internal control systems, it is imperative that they be protected and reliable.

In response to the growing concerns about the reliabilities of systems, the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) developed Trust Services, which incorporate "SysTrust" and "WebTrust" assurance services (AICPA 2003). These are professional assurance services provided by CPAs and CAs, aiming to report on the reliability and the risk of an information system. As stated earlier, based on the principles and criteria in the Trust Services, this study develops a comprehensive analytical formula for systems security risk for planning and evaluation purposes under DS theory of belief functions (Shafer 1976).

The AICPA/CICA (2003) SysTrust service has established principles and criteria for evaluating information system reliability. However, it does not provide much guidance as to how items of evidence pertaining to various principles, and criteria ought to be combined to determine whether these principles or criteria have been met. In addition, it does not provide any guidance on how judgments about the level of threats identified and the effectiveness of controls related to those threats ought to be combined. Therefore, it is difficult to assess the overall risk associated with whether the criteria or principles have been met.

Sun et al. (2006) use an evidential reasoning approach to evaluate information system security risk under DS theory. However, an analytical formula to combine all items of evidence at different levels is still missing in the information systems security risk literature. This paper tries to fill the void by developing a general analytical formula that incorporates the threats, vulnerabilities and controls, identified in the Trust Services as principles, sub-principles, and sub-sub-principles. The use of an analytical formula for systems security risk would not only facilitate the assessment of the overall system security risk pertaining to a criterion or principle, but would also provide an effective and efficient approach for planning and evaluation of information systems security and reliability.

The remainder of the paper is organized into seven sections. Section 2 provides a brief introduction to DS theory. Section 3 illustrates the framework for Trust Services based on principles and criteria established by AICPA/CICA (2003). Section 4 provides the details of the derivation of the general formulas for the systems security risk and systems reliability. Section 5 develops the specific analytical formulas for assessing systems security risk and reliability. Section 6 discusses the use of analytical formulas for planning and evaluation of systems security risk and systems reliability. Section 7 performs a comparison of the analytical formula based on a tree-structured evidential diagram with the model based on the network-structured evidential diagram. Finally, Section 8 summarizes the findings.

DEMPSTER-SHAFER THEORY OF BELIEF FUNCTIONS

Dempster-Shafer theory of belief functions has been applied to auditing and many other business and non-business areas (e.g., see Srivastava and Mock 2002). For example, Srivastava and Shafer (1992) apply DS theory to audit risk assessment. Srivastava and Datta (2002) apply the theory for evaluating mergers and acquisitions candidates. Shenoy and Shenoy (2002) demonstrate how the theory can be applied to evaluate financial portfolios. Bovee, Srivastava and Mak (2003) use the theory for assessing the quality of information. Srivastava, Buche, and Roberts (2005) apply the theory to evidential reasoning in causal maps. Recently, Srivastava, Mock and Turner (2007) use the theory to develop formulas for assessing fraud risk in financial statements audits, auditor independence risk on an audit engagement, and for assessing internal audit function by the external auditor. For the benefit of readers, we provide here the most essential concepts of DS theory. There are three basic functions that are important for the current study: *basic belief mass function*[2] *or m-values, belief function,* and *plausibility function*. We first briefly describe them below and then illustrate Dempster's rule of combination using a numerical example.

[2] Shafer (1976) calls it *basic probability assignment function*.

The Basic Belief Mass Function

The primary difference between the *basic belief mass function*, (i.e., m-values), and probabilities is that probabilities are assigned to individual elements or states of a frame, Θ, consisting of mutually exclusive and collectively exhaustive set of states. The sum of all such probabilities is one. The m-values in DS theory represent the uncertainties assigned to individual elements or states and to a set consisting of any two elements, three elements, and so on, to the entire frame (Shafer 1976). Similar to probabilities, all these m-values add up to one, i.e., $\sum_{A \subseteq \Theta} m(A) = 1$, where A represents a subset of the frame Θ, and the m-value for the empty set is 0, i.e., m(∅) = 0.

Belief Functions

The belief in a subset of a frame Θ, say A, is equal to the sum of all m-values for the individual elements in the subset A and the m-value on the subset A itself: $\mathrm{Bel}(A) = \sum_{B \subseteq A} m(B)$, where B is any subset of A. Belief in the empty set is 0, i.e., Bel(∅) = 0. A belief of zero in a statement or assertion implies that we do not have any evidence in support of the statement or assertion, whereas a zero probability in a state implies impossibility of the state. Similar to probability theory, a belief of one in a state, say A, i.e., Bel(A) = 1, represents certainty; A is true for certain.

Plausibility Functions

The plausibility in a subset of a frame, Θ, say A, represents the maximum uncertainty that could be assigned to A if all future evidence supported A. Mathematically one can express plausibility in A as: $\mathrm{Pl}(A) = \sum_{A \cap B \neq \emptyset} m(B) = 1\text{-}\mathrm{Bel}(\sim A)$. A plausibility of zero in a state implies that its negation is true for certain. In other words, if Pl(A) = 0 then, by definition, we have Bel(~A) = 1, which says that '~A' is true for sure.

To illustrate the basic concepts of belief functions, let us consider the following example. Suppose the auditor wants to assess the effectiveness of a security system pertaining to a client's information system. First, he/she will examine the company's policies and procedures related to the security system. Based on the evaluation of the policies and procedures, let us assume that the auditor derives the following levels of support. A low level of support, say 0.2 on a scale of 0−1, that the client's information system is protected against unauthorized access (*s*). A zero level of support represents that the system is not protected against unauthorized access (~*s*), i.e., there is no evidence based on the evaluations of the policies and procedures that the system is not protected against unauthorized access. And, 0.8 level of support remains uncommitted. This uncommitted part of uncertainty implies that the auditor is not sure whether 0.8 should be assigned to '*s*' or to '~*s*'. The auditor needs to collect more evidence. Under DS theory, the auditor's judgment can be represented in terms of the following m-values for the corresponding states, '*s*', '~*s*', and the frame $\{ s, \sim s\}$: m(*s*) = 0.2, m(~*s*) = 0, and m($\{s, \sim s \}$) = 0.8, where '*s*' represents the system is protected against unauthorized access, and '~*s*' represents the system is not protected against unauthorized access.

Based on the definition of belief functions, we have: Bel(*s*) = m(*s*) = 0.2, and Bel(~*s*) = m(~*s*) = 0, and Bel($\{s, \sim s\}$) = m(*s*) + m(~*s*) + m($\{s, \sim s\}$) = 0.2 + 0 + 0.8 = 1.

The corresponding plausibilities are:

$\text{Pl}(s) = \text{m}(s) + \text{m}(\{s, \sim s\}) = 0.2 + 0.8 =1$,

$\text{Pl}(\sim s) = \text{m}(\sim s) + \text{m}(\{s, \sim s\}) = 0 + 0.8 = 0.8$.

The plausibility that the system is not protected against unauthorized access, Pl(~*s*), defines the security risk as discussed later.

Dempster's Rule

Similar to Bayes' rule in probability theory, Dempster's rule in DS theory is used to combine independent items of evidence pertaining to a variable. In fact, Dempster's rule becomes Bayes' rule under the condition where we have belief masses distributed only over the single elements of the frame of a variable. We use a numerical example to illustrate Dempster's rule next.

Let us consider the previous example of whether the system is secure from unauthorized access (S) with two possible values '*s*' and '~*s*', representing that the system is secure and is not secure, respectively, against unauthorized access. In addition, let us assume that the auditor has obtained and assessed two independent items of evidence pertaining to the variable S with the following sets of m-values:

Evidence 1: $m_1(s) = 0.2$, $m_1(\sim s) = 0$, $m_1(\{(s, \sim s\}) = 0.8$ (as assumed earlier),

Evidence 2: $m_2(s) = 0.6$, $m_2(\sim s) = 0.1$, $m_2(\{(s, \sim s\}) = 0.3$ (new piece of evidence).

The above m-values imply that Evidence 1 provides 0.2 level of support, on a scale 0−1, that '*s*' is true, no support for '~*s*', and 0.8 level of support uncommitted, and Evidence 2 provides 0.6 level of support that '*s*' is true, 0.1 level of support that '~*s*' is true and 0.3 level of support uncommitted.

The question we want to answer is what is the combined belief mass function? Dempster's rule determines the answer. In general, for two items of evidence pertaining to a variable with the frame Θ, Dempster's rule can be expressed as:

$$m(A) = (1/K)\Sigma\{m_1(A1)m_2(A2)|A1\cap A2 = A, A\neq\varnothing\},$$

where m(A) is the resultant m-value for the subset A of the frame Θ, m_1 and m_2 are the two sets of m-values associated with the two independent items of evidence, and K is the renormalization constant given as:

$$K = 1 - \Sigma\{m_1(A1)m_2(A2)|A1 \cap A2 = \varnothing\}.$$

The second term in K represents the conflict between the two items of evidence. For Dempster's rule with more than two items of evidence see Shafer (1976).

For our example, the renormalization constant is:

$$K = 1 – [m_1(s)m_2(\sim s) + m_1(\sim s)m_2(s)] = 1 – [(0.2)(0.1) + (0)(0.6)] = 0.98,$$

and the combined m-values are:

$$m(s) = [m_1(s)m_2(s) + m_1(s)m_2(\{s, \sim s\}) + m_1(\{s, \sim s\})m_2(s)]/K$$

$$= [(0.2)(0.6) + (0.2)(0.3) +(0.8)(0.6)]/0.98 = 0.673,$$

$$m(\sim s) = [m_1(\sim s)m_2(\sim s) + m_1(\sim s)m_2(\{s, \sim s\}) + m_1(\{s, \sim s\})m_2(\sim s)]/K$$

$$= [(0)(0.1) + (0)(0.3) +(0.8)(0.1)]/0.98 = 0.082,$$

$$m(\{s, \sim s\}) = m_1(\{s, \sim s\})m_2(\{s, \sim s\})/K = (0.8)(0.3)/0.98 = 0.245.$$

Basically, Dempster’s rule dictates that the state ‘*s*’ is true, i.e., the system is protected against unauthorized access when both items of evidence affirm that ‘*s*’ is true or one item of evidence affirms ‘*s*’ and the other one is ambiguous about it. Similarly, ‘~*s*’ is true when both items of evidence affirm it or when one affirms it and the other one is ambiguous about it. However, when one item of evidence affirms a state and the other one negates it, this represents a conflict in the evidence. This conflict is eliminated and the combined m-values are renormalized to add to one, as shown above.

Measure of Risk and Reliability of Systems Security under DS Theory

Srivastava and Shafer (1992) argue that the plausibility that material errors exist in the financial statements defines the audit risk. Similarly, we argue that the plausibility that a given principle is not met represents the risk associated with that principle. For example, the systems security risk can be defined as the plausibility that the system is not protected against unauthorized access given the evidence collected, i.e.:

$$\text{Systems Security Risk} = \text{Pl}(\sim s).$$

The definition of risk using plausibility function under belief functions provides a conservative (worst-case scenario) measure of risk. For the example given above, in Evidence 1, even though we do not have any support for '$\sim s$' (the system is not protected against unauthorized access), i.e., $\text{m}(\sim s) = 0$, or $\text{Bel}(\sim s) = 0$, the plausibility that the system is not protected is 0.8, i.e., $\text{Pl}(\sim s) = 0.8$. $\text{Pl}(\sim s)$ represents the potential risk or the risk that the system is not secure given the evidence collected.

The measure of reliability that the system is secure against unauthorized access can be defined in terms of the belief that the system is secure from unauthorized access, i.e.,

$$\text{Systems Security Reliability} = \text{Bel}(s)$$

For the above example, since $\text{Bel}(s) = 0.2$, the systems security reliability is 0.2.

FRAMEWORK FOR TRUST SERVICES

Trust Services framework identified by AICPA/CICA (2003) include five principles underlying reliable business systems, including e-commerce systems:

1. Security: The system is protected against unauthorized access (both physical and logical).
2. Availability: The system is available for operation and use as committed or agreed.
3. Processing Integrity: System processing is complete, accurate, timely, and authorized.

4. Online Privacy: Personal information obtained as a result of e-commerce is collected, used, disclosed, and retained as committed or agreed.
5. Confidentiality: Information designated as confidential is protected as committed or agreed.

As stated earlier, the risk formulas for all five principles follow the same analytical process. While we develop general formulas for risks and reliabilities for a generic principle, we focus our analysis to the "Systems Security" principle. The formulas for the other four principles can be derived easily from the general formulas as presented in the next section.

Table 1 describes the Security principle along with its related sub-principles and sub-sub-principles. This table is created from the AICPA (2003) publication on Trust Services. Column 1 of Table 1 lists the main principle, Security. Column 2 lists the corresponding sub-principles. Column 3 lists all the sub-sub-principles. The assessment of the security risk is operationalized through an evidential diagram (Sun et al. 2006). We develop an evidential diagram in Figure 1 related to "Security" principle. This diagram is based on the AICPA publication (AICPA 2003) for the items of evidence pertaining to Security principle, sub-principles and sub-sub-principles.

------ Table 1 about here ------

As mentioned above, Figure 1 represents an evidential diagram for the principle "System Security", which implies that the system is protected against unauthorized access. The rounded boxes in Figure 1 represent variables, and the rectangular boxes represent items of evidence. The main principle, sub-principles, and sub-sub-principles are the variables, which take values. In our case, we assume all the variables to be binary as assumed by previous researchers (see, e.g., Srivastava and Shafer 1992), which means either they are true or not true. Some items of evidence pertain to more than one variable, for example, "identification and documentation of the security requirements of authorized users" pertain to two sub-sub-principles: "procedures exist to ensure systems are protected against unauthorized logical access" and "policies exist to ensure systems are protected against unauthorized physical access" (see Figure 1). Consequently, the evidential diagram becomes a network (e.g., Srivastava et al. 1996, Mock et al. 1998; Srivastava and Lu 2002).

----- Figure 1 about here -----

In Figure 1, the variable "System Security (S)" is connected through an "AND" relationship, represented by a circle with "&", to the three variables representing sub-principles: "Protection against unauthorized logical access (L)", "Protection against unauthorized physical access (P)", and "Protection against infection by computer viruses (V)". The "and" relationship implies that the main principle, "System Security", is true if and only if the three sub-principles are met. These sub-principles are derived from the principles of "System Security" in Trust Services. As mentioned earlier, rectangular boxes in Figure 1 represent evidence nodes, representing sets of audit procedures as described in the corresponding evidence nodes. The procedures described in the evidence nodes are not meant to be exhaustive. In Figure 1, the evidence nodes pertaining to a particular variable are connected by a line to the corresponding variable or variables. The number in each evidence node represents the level of support in favor of the assertion or sub-assertion it pertains to. If an item of evidence pertains to more than one assertion or sub-assertion, the number represents the level of support in favor of all the assertions or sub-assertions it pertains to. It should be noted that the level of support in favor of the negation of the assertion or sub-assertion is assumed to be zero for all the evidence depicted in Figure 1 and Figure 2. However, for the analysis purposes as presented later, we relax this assumption and consider mixed items of evidence.

As discussed earlier, the evidential diagram in Figure 1 is a network. Developing analytical formulas for such a network becomes very complex. Similar to Srivastava and Shafer (1992) for the audit risk formula for financial audits, we develop the analytical formula for the systems security risk for "SysTrust" services for a tree-type evidential diagram as given in Figure 2. However, in our case to derive the formulas, we had to convert the evidential diagram in Figure 1 from a network structure to a tree structure as shown in Figure 2, by splitting an item of evidence pertaining to two variables, into two separate items of evidence, each pertaining to one of the two variables. It is important to note that in the process of splitting, we maintain the original strength of the evidence pertaining to each individual variable. As discussed later in the section on comparison of systems security risk formula with the network model, the impact of this splitting is that the overall belief that the systems is secure is lower in the tree model than what it is in the network model, and the belief that systems is not secure is higher for the tree model than the value for the network model. These results yield a conservative estimate of the systems security risk.

----- Figure 2 about here -----

GENERAL SYSTEMS SECURITY RISK AND RELIABILITY FORMULAS

In this section, we develop general formulas for assessing the systems security risk and the systems security reliability in terms of the three sub-principles - protection against unauthorized logical access (L), protection against unauthorized physical access (P), and protection against infection by computer viruses (V) - for the evidential diagram depicted in Figure 3. This evidential diagram is assumed to be a tree for deriving analytical formulas. As mentioned earlier, developing analytical formulas for network type evidential diagrams is very complex. We consider a general case where we have multiple items of evidence for each variable; variables being the main principle, sub-principles, and the sub-sub-principles.[3] The number of independent items of evidence for each variable is denoted by the symbol "q" with a subscript representing the specific variable. For example, q_{LP} represents the number of independent items of evidence for the sub-sub-principle LP (see Table 2). Specific formulas are derived in the following section using the general results derived in this section.

----- Figure 3 about here ----

We use upper case letters to represent the names of the variables in the evidential diagram and lower case letters to represent their values. For example, we represent the sub-principle "Protection against unauthorized physical access" by "P" and its values by "*p*" and "*~p"*', representing, respectively, that the system is protected against unauthorized physical access and that the system is not protect against unauthorized physical access. Table 2 lists detailed symbols and their definitions.

As mentioned earlier, we use the belief-function definition of risk as defined by Srivastava and Shafer (1992) in terms of the plausibility function. For example, the overall risk that the system is not secure can be expressed as the total plausibility, $\mathrm{Pl}_{\mathrm{Total}}(\sim s)$, that the system is not secure after considering all the evidence gathered in the process. Since $\mathrm{Pl}_{\mathrm{Total}}(\sim s) = \mathrm{m}_{\mathrm{Total}}(\sim s) + \mathrm{m}_{\mathrm{Total}}(\{s, \sim s\})$, we need to determine the total m-values at the variable S in Figure 3. To achieve this objective, we use the following steps. First, we combine all the multiple items of evidence pertaining to a variable and obtain a belief mass function at each variable. These belief mass functions are represented by m-values with a subscript representing the name of the variable. For example, the combined belief mass function at LP is represented by the following

[3] One can easily extend the analytical formulas derived here to the most general case where we have not only multiple items of evidence for each principle, sub-principle, and sub-sub-principle but also have multiple sub-principles, and multiple other sub-levels of principles.

set of belief masses: $m_{LP}(lp)$, $m_{LP}(\sim lp)$, and $m_{LP}(\{lp, \sim lp\})$. Second, we propagate belief masses from the sub-sub-principle level to the sub-principle level. Third, we combine the propagated belief from the sub-sub-principles to the sub-principle level with the belief masses obtained at each sub-principle as a result of direct evidence pertaining to the sub-principle. Finally, we propagate the resulting belief masses from the sub-principle level to the main principle. Then we combine these belief masses with the belief masses obtained at the main principle as a result of direct evidence at the main principle. This process yields the total belief mass function at the main principle, which yields the desired formula for the system security risk and the systems security reliability. The above steps are described below in detail.

Step 1: Combine multiple items of evidence at each variable

As we see in Figure 3, each variable in the diagram has multiple independent items of evidence. The number of items at each variable is denoted by symbol "q" with a subscript representing the name of the variable. We illustrate the process of combining multiple items of evidence at each variable using the example of variable S. All the other cases are similar and the results are presented in Table 3.

We use Dempster's rule as simplified by Srivastava (2005) for binary variables to combine q_S items of evidence for variable S. Let us assume that the strengths of various items of evidence pertaining to S are given below in terms of belief masses, i.e., m-values, as:

Evidence 1: $m_1(s)$, $m_1(\sim s)$, $m_1(\{s,\sim s\})$

Evidence 2: $m_2(s)$, $m_2(\sim s)$, $m_2(\{s,\sim s\})$

………… ……………….

Evidence qs: $m_{q_S}(s)$, $m_{q_S}(\sim s)$, $m_{q_S}(\{s,\sim s\})$

Using Dempster's rule as simplified by Srivastava (2005, Equations 10-13) to combine the above m-values, we obtain the following set of belief masses at variable S:

$$m_S(s) = 1 - \prod_{i=1}^{q_S} (1 - m_i(s)) / K_S, \tag{1a}$$

$$m_S(\sim s) = 1 - \prod_{i=1}^{q_S} (1 - m_i(\sim s)) / K_S, \tag{1b}$$

$$m_S(\{s, \sim s\}) = \prod_{i=1}^{q_S} m_i(\{s, \sim s\}) / K_S, \tag{1c}$$

where K_S is given by

$$K_S = \prod_{i=1}^{q_S} (1 - m_i(s)) + \prod_{i=1}^{q_S} (1 - m_i(\sim s)) - \prod_{i=1}^{q_S} m_i(\{s, \sim s\}) \cdot \tag{1d}$$

Using the above approach we combine all the direct items of evidence at all the other variables. This process yields the belief masses at each variable as given in Table 3.

Step 2: Propagate belief masses from sub-sub-principle to sub-principle

In this step, we propagate the belief masses from the nine sub-sub-principles to their related sub-principles (L, P, and V) through an “AND” relational node (see Figure 3). We use Srivastava et al. (1995, Proposition 1) to achieve the above objective. In the present case, we have three sub-principles (L, P, and V). Thus, using Srivastava et al. (1995, Equations 1 and 2), we obtain the following set of m-values on “L” as a result of propagation from the associated three sub-sub-principle variables (LP, LC, and LR):

$$m_{L \leftarrow LP,LC,LR}(l) = m_{LP}(lp) m_{LC}(lc) m_{LR}(lr), \tag{2a}$$

$$m_{L \leftarrow LP, LC, LR}(\sim l) = 1 - [1 - m_{LP}(\sim lp)][1 - m_{LC}(\sim lc)][1 - m_{LR}(\sim lr)], \tag{2b}$$

$$m_{L \leftarrow LP, LC, LR}(\{l, \sim l\}) = 1 - m_{L \leftarrow LP, LC, LR}(l) - m_{L \leftarrow LP, LC, LR}(\sim l), \tag{2c}$$

where “L” represents “protection against unauthorized logical access”.

Again using Srivastava et al. (1995, Equations. 1 and 2) we obtain the following sets of m-values at nodes “P” and “V” as a result of propagation from their corresponding sub-sub-principles:

$$\mathrm{m}_{\mathrm{P}\leftarrow\mathrm{PP,PC,PR}}(p) = \mathrm{m}_{\mathrm{PP}}(pp)\mathrm{m}_{\mathrm{PC}}(pc)\mathrm{m}_{\mathrm{PR}}(pr), \tag{3a}$$

$$\mathrm{m}_{\mathrm{P}\leftarrow\ \mathrm{PP,\ PC,\ PR}}(\sim p) = 1\text{-}\ [1\text{-}\ \mathrm{m}_{\mathrm{PP}}(\sim pp)][1\text{-}\ \mathrm{m}_{\mathrm{PC}}(\sim pc)][1\text{-}\mathrm{m}_{\mathrm{PR}}(\sim pr)], \tag{3b}$$

$$\mathrm{m}_{\mathrm{P}\leftarrow\ \mathrm{PP,\ PC,\ PR}}(\{p, \sim p\}) = 1 - \mathrm{m}_{\mathrm{P}\leftarrow\ \mathrm{PP,\ PC,\ PR}}(p) - \mathrm{m}_{\mathrm{P}\leftarrow\mathrm{PP,PC,PR}}(\sim p), \tag{3c}$$

and

$$\mathrm{m}_{\mathrm{V}\leftarrow\mathrm{VP,VC,VR}}(v) = \mathrm{m}_{\mathrm{VP}}(vp)\mathrm{m}_{\mathrm{VC}}(vc)\mathrm{m}_{\mathrm{VR}}(vr), \tag{4a}$$

$$\mathrm{m}_{\mathrm{V}\leftarrow\mathrm{VP,\ VC,\ VR}}(\sim v) = 1 - [1 - \mathrm{m}_{\mathrm{VP}}(\sim vp)][1 - \mathrm{m}_{\mathrm{VC}}(\sim vc)]\ [1 - \mathrm{m}_{\mathrm{VR}}(\sim vr)], \tag{4b}$$

$$\mathrm{m}_{\mathrm{V}\leftarrow\mathrm{VP,\ VC,\ VR}}(\{v, \sim v\}) = 1 - \mathrm{m}_{\mathrm{V}\leftarrow\mathrm{VP,\ VC,\ VR}}(v)\ - \mathrm{m}_{\mathrm{V}\leftarrow\mathrm{VP,\ VC,\ VR}}(\sim v\ ), \tag{4c}$$

where “P’ denotes “protection against unauthorized physical access”; and “V” denotes “protection against infection by computer viruses”.

Step 3: Combine beliefs at the sub-principle level

We have two sets of belief masses or m-values at each sub-principle. One set comes from the evidence directly bearing on the sub-principle. The other set is the m-values propagated from the corresponding sub-sub-principles as obtained in Step 2 above. We use Dempster's rule again as simplified by Srivastava (2005) for binary variables to combine the two sets of m-values. The combined m-values at each sub-principle are given as:

<u>Sub-principle: Protection from Unauthorized Logical Access</u>

$$\mathrm{m'}_{\mathrm{L}}(l) = 1 - \prod_{\mathrm{i}=1}^{\mathrm{q_L}}(1 - \mathrm{m}_{\mathrm{Li}}(l))(1 - \mathrm{m}_{\mathrm{L}\leftarrow\mathrm{LP,LC,LR}}(l))\,/\,\mathrm{K_L}\,, \tag{5a}$$

$$\mathrm{m'}_{\mathrm{L}}(\sim l) = 1 - \prod_{\mathrm{i}=1}^{\mathrm{q_L}}(1 - \mathrm{m}_{\mathrm{Li}}(\sim l))(1 - \mathrm{m}_{\mathrm{L}\leftarrow\mathrm{LP,LC,LR}}(\sim l))\,/\,\mathrm{K_L}\,, \tag{5b}$$

$$\mathrm{m'}_{\mathrm{L}}(\{l, \sim l\}) = \prod_{\mathrm{i}=1}^{\mathrm{q_L}}\mathrm{m}_{\mathrm{Li}}(\{l, \sim l\})\mathrm{m}_{\mathrm{L}\leftarrow\mathrm{LP,LC,LR}}(\{l, \sim l\})\,/\,\mathrm{K_L}\,, \tag{5c}$$

where

$$\mathrm{K_L} = \prod_{\mathrm{i=1}}^{\mathrm{q_L}} (1 - \mathrm{m_{Li}}(l))(1 - \mathrm{m_{L\leftarrow LP,LC,LR}}(l)) + \prod_{\mathrm{i=1}}^{\mathrm{q_L}} (1 - \mathrm{m_{Li}}(\sim l))(1 - \mathrm{m_{L\leftarrow LP,LC,LR}}(\sim l))$$

$$- \prod_{\mathrm{i=1}}^{\mathrm{q_L}} \mathrm{m_{Li}}(\{l, \sim l\}) \mathrm{m_{L\leftarrow LP,LC,LR}}(\{l, \sim l\}) . \qquad \text{(5d)}$$

Sub-Principle: Protection from Unauthorized Physical Access

$$\mathrm{m'_P}(p) = 1 - \prod_{\mathrm{i=1}}^{\mathrm{q_P}} (1 - \mathrm{m_{Pi}}(p))(1 - \mathrm{m_{P\leftarrow PP,PC,PR}}(p)) / \mathrm{K_P} , \qquad \text{(6a)}$$

$$\mathrm{m'_P}(\sim p) = 1 - \prod_{\mathrm{i=1}}^{\mathrm{q_P}} (1 - \mathrm{m_{Pi}}(\sim p))(1 - \mathrm{m_{P\leftarrow PP,PC,PR}}(\sim p)) / \mathrm{K_P} , \qquad \text{(6b)}$$

$$\mathrm{m'_P}(\{p, \sim p\}) = \prod_{\mathrm{i=1}}^{\mathrm{q_P}} \mathrm{m_{Pi}}(\{p, \sim p\}) \mathrm{m_{P\leftarrow PP,PC,PR}}(\{p, \sim p\}) / \mathrm{K_P} , \qquad \text{(6c)}$$

where

$$\mathrm{K_P} = \prod_{\mathrm{i=1}}^{\mathrm{q_P}} (1 - \mathrm{m_{Pi}}(p))(1 - \mathrm{m_{P\leftarrow PP,PC,PR}}(p)) + \prod_{\mathrm{i=1}}^{\mathrm{q_P}} (1 - \mathrm{m_{Pi}}(\sim p))(1 - \mathrm{m_{P\leftarrow PP,PC,PR}}(\sim p))$$

$$- \prod_{\mathrm{i=1}}^{\mathrm{q_P}} \mathrm{m_{Pi}}(\{p, \sim p\}) \mathrm{m_{P\leftarrow PP,PC,PR}}(\{p, \sim p\}) . \qquad \text{(6d)}$$

Sub-Principle: Protection from Computer Viruses

$$\mathrm{m'_V}(v) = 1 - \prod_{\mathrm{i=1}}^{\mathrm{q_V}} (1 - \mathrm{m_{Vi}}(v))(1 - \mathrm{m_{V\leftarrow VP,VC,VR}}(v)) / \mathrm{K_V} , \qquad \text{(7a)}$$

$$\mathrm{m'_V}(\sim v) = 1 - \prod_{\mathrm{i=1}}^{\mathrm{q_V}} (1 - \mathrm{m_{Vi}}(\sim v))(1 - \mathrm{m_{V\leftarrow VP,VC,VR}}(\sim v)) / \mathrm{K_V} , \qquad \text{(7b)}$$

$$\mathrm{m'_V}(\{v, \sim v\}) = \prod_{\mathrm{i=1}}^{\mathrm{q_V}} \mathrm{m_{Vi}}(\{v, \sim v\}) \mathrm{m_{V\leftarrow VP,VC,VR}}(\{v, \sim v\}) / \mathrm{K_V} , \qquad \text{(7c)}$$

$$\mathrm{K_V} = \prod_{\mathrm{i=1}}^{\mathrm{q_V}} (1 - \mathrm{m_{Vi}}(v))(1 - \mathrm{m_{V\leftarrow VP,VC,VR}}(v)) + \prod_{\mathrm{i=1}}^{\mathrm{q_V}} (1 - \mathrm{m_{Vi}}(\sim v))(1 - \mathrm{m_{V\leftarrow VP,VC,VR}}(\sim v))$$

$$- \prod_{\mathrm{i=1}}^{\mathrm{q_V}} \mathrm{m_{Vi}}(\{v, \sim v\}) \mathrm{m_{V\leftarrow VP,VC,VR}}(\{v, \sim v\}) \qquad \text{(7d)}$$

Step 4: Propagate beliefs from sub-principles to main principle

In this step, we propagate m-values from the three sub-principles (L, P, and V) to the main principles (S) through an “AND” relational node. We use Srivastava et al. (1995, Proposition 1) again to achieve the above objective.

$$\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(s) = \mathrm{m'}_{\mathrm{L}}(l)\mathrm{m'}_{\mathrm{P}}(p)\mathrm{m'}_{\mathrm{V}}(v), \tag{8a}$$

$$\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(\sim s) = 1-[1\text{-}\mathrm{m'}_{\mathrm{L}}(\sim l)][1\text{-}\mathrm{m'}_{\mathrm{P}}(\sim p)][1\text{-}\mathrm{m'}_{\mathrm{V}}(\sim v)], \tag{8b}$$

$$\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(\{s, \sim s\}) = 1- \mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,V}}(s) - \mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(\sim s), \tag{8c}$$

where "*s*" denotes "system is protected against unauthorized access" and "~s" denotes that the system is not protected against unauthorized access.

Step 5: Combination of m-values at the main principle

This step is the final step in deriving the systems security risk and systems security reliability formulas. In order to achieve our goal, we need to combine all the evidence (i.e., the corresponding m-values) at the main principle. In our example in Figure 3, we have two sets of m-values at the main principle. One set of m-values come from the evidence directly bearing on the main principle. The other set comes from the m-values propagated to the main principle from the sub-principles, as shown in Step 4. The combined belief masses originating from the direct evidence at S were determined in Step 1 as given in (1). The next step is to combine the belief masses given in (1) with the belief masses propagated from L, P, and V, to S, as given in (8) using Dempster's rule. The combined belief masses, i.e., the total m-values, at S are given below using Srivastava (2005) representation:

$$\mathrm{m}_{\mathrm{Total}}(s) = 1-[1-\mathrm{m}_{\mathrm{S}}(s)][1-\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(s)]/\mathrm{K}, \tag{9a}$$

$$\mathrm{m}_{\mathrm{Total}}(\sim s) = 1-[1-\mathrm{m}_{\mathrm{S}}(\sim s)][1-\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(\sim s)]/\mathrm{K},, \tag{9b}$$

$$\mathrm{m}_{\mathrm{Total}}(\{s,\sim s\}) = \mathrm{m}_{\mathrm{S}}(\{s,\sim s\})\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(\{s,\sim s\})/\mathrm{K}, \tag{9c}$$

where K is the renormalization constant in Dempster's rule and given by the following expression:

$$\mathrm{K} = 1 - [\mathrm{m}_{\mathrm{S}}(s)\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(\sim s) + \mathrm{m}_{\mathrm{S}}(\sim s)\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(s)]. \tag{9d}$$

From (9), we obtain the following expressions for the total belief that the system is protected against unauthorized access, and the total belief and plausibility that the system is not protected against unauthorized access:

$$\mathrm{Bel}_{\mathrm{Total}}(s) = \text{Systems Security Reliability} = 1-[1-\mathrm{m}_{\mathrm{S}}(s)][1-\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(s)]/\mathrm{K} \tag{10}$$

$$\mathrm{Bel}_{\mathrm{Total}}(\sim s) = 1-[1-\mathrm{m}_{\mathrm{S}}(\sim s)][1-\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(\sim s)]/\mathrm{K} \tag{11}$$

$$\mathrm{Pl}_{\mathrm{Total}}(\sim s) = \text{Systems Security Risk} = [1-\mathrm{m}_{\mathrm{S}}(s)][1-\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,\,P,\,V}}(s)]/\mathrm{K} \tag{12}$$

Equation (12) represents the overall plausibility or risk that the system is not secure given all the evidence we have gathered at various levels. The belief mass, $\mathrm{m}_{\mathrm{S}}(s)$, is defined in (1), $\mathrm{m}_{\mathrm{S}\leftarrow\mathrm{L,P,V}}(s)$ in (8), and K is defined in (9d). The formulas for the systems reliability in (10) and the systems security risk in (12) are general formulas in terms of specific belief masses obtained from various items of evidence at different levels. They are valid even in those situations where the evidence may be conflicting. Similar to the above derivation, one can easily derive general formulas for the other four main principles of SysTrust services.

SPECIFIC SYSTEMS SECURITY RISK AND RELIABILITY FORMULAS

In this section we derive the formulas for assessing systems security risk and reliability for the evidential diagram given in Figure 2 using the general formula derived in the previous section. The formulas derived in the previous section assume multiple items of evidence at each level in the evidential diagram (see Figure 3). For the present case, we have either one or two items of evidence per variable, variable being the main principle, sub-principles, or sub-sub-principles. To derive the systems security risk and reliability formulas for the evidential diagram in Figure 2 using the general result in (10, 12), we set the number of items of evidence for each variable as follows: $\mathrm{q}_{\mathrm{S}} = 1$, $\mathrm{q}_{\mathrm{L}} = 1$, $\mathrm{q}_{\mathrm{P}} = 1$, $\mathrm{q}_{\mathrm{V}} = 1$, $\mathrm{q}_{\mathrm{LP}} = 2$, $\mathrm{q}_{\mathrm{LC}} = 1$, $\mathrm{q}_{\mathrm{LR}} = 1$, $\mathrm{q}_{\mathrm{PP}} = 1$, $\mathrm{q}_{\mathrm{PC}} = 1$, $\mathrm{q}_{\mathrm{PR}} = 2$, $\mathrm{q}_{\mathrm{VP}} = 2$, $\mathrm{q}_{\mathrm{VC}} = 1$, and $\mathrm{q}_{\mathrm{VR}} = 2$ (See Table 2 for definitions). From Equations (10) and (12) and using (1) - (9), we obtain the following formula for assessing the systems security risk and systems security reliability for evidential diagram in Figure 2:

$$\text{Systems Security Risk} = \mathrm{Pl}_{\mathrm{Total}}(\sim s) = [1-\mathrm{m}_{\mathrm{S}}(s)][1-\mathrm{m}_{\mathrm{S}\leftarrow \mathrm{L, P, V}}(s)]/\mathrm{K}, \tag{13}$$

$$\text{Systems Security Reliability} = \mathrm{Bel}_{\mathrm{Total}}(\mathrm{s}) = 1 - [1-\mathrm{m}_{\mathrm{S}}(s)][1-\mathrm{m}_{\mathrm{S}\leftarrow \mathrm{L, P, V}}(s)]/\mathrm{K}, \tag{14}$$

$$\mathrm{K} = 1 - [\mathrm{m}_{\mathrm{S}}(s)\mathrm{m}_{\mathrm{S}\leftarrow \mathrm{L, P, V}}(\sim s) + \mathrm{m}_{\mathrm{S}}(\sim s)\mathrm{m}_{\mathrm{S}\leftarrow \mathrm{L, P, V}}(s)]. \tag{15}$$

where K is the renormalization constant in Dempster's rule as the result of conflicting items of evidence. $\mathrm{m}_{\mathrm{S}}(s)$ and $\mathrm{m}_{\mathrm{S}}(\sim s)$, respectively, represent the level of support for “*s*” and “~*s*” that the system is secure and that the system is not secure, respectively, against unauthorized access based on the evidence pertaining to variable S in Figure 2. $\mathrm{m}_{\mathrm{S}\leftarrow \mathrm{L, P, V}}(s)$ and $\mathrm{m}_{\mathrm{S}\leftarrow \mathrm{L, P, V}}(\sim s)$, respectively, represent the level of support for “*s*” and “~s” obtained as the result of combining information, i.e., belief masses, from the sub-principles L, P, and V. These belief masses are defined as (see 8):

$$\mathrm{m}_{\mathrm{S}\leftarrow \mathrm{L, P, V}}(s) = \mathrm{m'}_{\mathrm{L}}(l)\mathrm{m'}_{\mathrm{P}}(p)\mathrm{m'}_{\mathrm{V}}(v), \tag{16a}$$

$$\mathrm{m}_{\mathrm{S}\leftarrow \mathrm{L, P, V}}(\sim s) = 1-[1-\mathrm{m'}_{\mathrm{L}}(\sim l)][1-\mathrm{m'}_{\mathrm{P}}(\sim p)][1-\mathrm{m'}_{\mathrm{V}}(\sim v)], \tag{16b}$$

where

$$\mathrm{m'}_{\mathrm{L}}(l) = 1-[1-\mathrm{m}_{\mathrm{L}}(l)][1-\mathrm{m}_{\mathrm{L}\leftarrow \mathrm{LP,LC,LR}}(l)]/\mathrm{K}_{\mathrm{L}}, \tag{17a}$$

$$\mathrm{m'}_{\mathrm{L}}(\sim l) = 1-[1-\mathrm{m}_{\mathrm{L}}(\sim l)][1-\mathrm{m}_{\mathrm{L}\leftarrow \mathrm{LP,LC,LR}}(\sim l)]/\mathrm{K}_{\mathrm{L}}, \tag{17b}$$

$$\mathrm{m'}_{\mathrm{P}}(p) = 1-[1-\mathrm{m}_{\mathrm{P}}(p)][1-\mathrm{m}_{\mathrm{P}\leftarrow \mathrm{PP,PC,PR}}(p)]/\mathrm{K}_{\mathrm{P}}, \tag{18a}$$

$$\mathrm{m'}_{\mathrm{P}}(\sim p) = 1-[1-\mathrm{m}_{\mathrm{P}}(\sim p)][1-\mathrm{m}_{\mathrm{P}\leftarrow \mathrm{PP,PC,PR}}(\sim p)]/\mathrm{K}_{\mathrm{P}}, \tag{18b}$$

$$\mathrm{m'}_{\mathrm{V}}(v) = 1-[1-\mathrm{m}_{\mathrm{V}}(v)][1-\mathrm{m}_{\mathrm{V}\leftarrow \mathrm{VP,VC,VR}}(v)]/\mathrm{K}_{\mathrm{V}}, \tag{19a}$$

$$\mathrm{m'}_{\mathrm{V}}(\sim v) = 1-[1-\mathrm{m}_{\mathrm{V}}(\sim v)][1-\mathrm{m}_{\mathrm{V}\leftarrow \mathrm{VP,VC,VR}}(\sim v)]/\mathrm{K}_{\mathrm{V}}. \tag{19b}$$

The belief masses represented by $m_L(l)$, $m_L(\sim l)$, $m_P(p)$, $m_P(\sim p)$, and $m_V(v)$ and $m_V(\sim v)$, respectively, represent the level of support from the respective evidence in Figure 2 in favor of and against the corresponding variable. The belief masses, $m_{L\leftarrow LP,LC,LR}(l)$, $m_{L\leftarrow LP,LC,LR}(\sim l)$, $m_{P\leftarrow PP,PC,PR}(p)$, $m_{P\leftarrow PP,PC,PR}(\sim p)$, $m_{V\leftarrow VP,VC,VR}(v)$, and $m_{V\leftarrow VP,VC,VR}(\sim v)$, along with the corresponding Ks are given in Table 4.

----- Table 4 about here -----

Equation (13) represents the systems security risk for the evidential diagram in Figure 2. It is worth noting that the overall risk in (13) is the product of two risks. While $[1- m_S(s)]$ represents the risk or plausibility that the system is not secure based on the evidence directly pertaining to S, $[1- m_{S\leftarrow L,P,V}(s)]$ represents the risk or plausibility that the system is not secure from unauthorized access based on all the information relevant to other variables. The constant K in (13, see also 15) arises due to the conflicting information between the two sources, one directly bearing on S and the other coming from the sub-principles L, P, and V. We further analyze the formula in (13) in the next section when we compare its performance with the network results for various input beliefs in terms of m-values. The assurance provider can program (13) in a spreadsheet and use it to plan and evaluate assurance engagements.

When the assurance provider is planning for the assurance service, he/she usually plans with affirmative items of evidence. Such items of evidence provide support only for the affirmation of the variables. In such a situation, we will have a zero belief mass assigned to the negation of the variable. For example, in such a situation, we will have a zero value for the following m-values: $m_S(\sim s) = m_L(\sim l) = m_P(\sim p) = m_V(\sim v) = m_{LP1}(\sim lp) = m_{LP2}(\sim lp) = m_{LC}(\sim lc) = m_{LR}(\sim lr) = m_{PP}(\sim pp) = m_{PC}(\sim pc) = m_{PR1}(\sim pr) =m_{PR2}(\sim pr) = m_{VP1}(\sim vp) = m_{VP2}(\sim vp) = m_{VC}(\sim vc) = m_{VR1}(\sim vr) = m_{VR2}(\sim vr) = 0$. This assumption yields K=1, and also all the renormalization constants given in Table 4 become unity. This case is similar to the situation assumed by Srivastava and Shafer (1992) for their derivation of the audit risk formula for financial audits. Our formula in (13) is a general result in the sense that it incorporates positive, negative or mixed items of evidence, whereas the Srivastava and Shafer (1992) audit risk formula is only valid for affirmative, i.e., positive items of evidence.

PLANNING AND EVALUATION OF ASSURANCE SERVICES

Planning Systems Security Assessment Engagement

Similar to the Audit Risk model of SAS 47 (AICPA 1983 see also the revised standard SAS 106, AICPA 2006) being used for planning financial audit engagements; systems security risk formula derived in Equation (13) can be used for planning the assurance engagement for systems security risk assessment. The assurance provider can start the planning process by first developing an evidential diagram similar to Figure 2 that is pertinent to the engagement and by recognizing the appropriate items of evidence pertaining to various assertions (principles, sub-principles, and sub-sub-principles). Next, the assurance provider can plan for the level of support he/she would like to obtain from various items of evidence for the corresponding assertions (i.e., principles, sub-principles, and sub-sub-principles). The systems security risk formula in (13) can be used to determine the overall systems security risk by inputting the belief masses, i.e., m-values, planned to be obtained from each item of evidence. The systems security risk formula will give the overall risk that the assurance provider will achieve if each item of evidence provides the planned level of support. The desired level of support to be obtained from each item of evidence will depend on the nature, timing, and extent of the procedure and on the cost of performing the procedures. One can easily develop a spreadsheet program either in MS Excel or Lotus to calculate the overall information systems security risk using Equation (13).

Evaluation of Systems Security Risk or Reliability

Equations (13) and (14) can be used for evaluating systems security risk and systems security reliability. As mentioned above, the assurance provider would have already developed an evidential diagram and identified various items of evidence pertaining to various assertions during the planning phase. Once the assurance provider has performed various audit procedures and assessed the level of support related to whether the corresponding assertion is met or not met, he/she can input these judgments into Equations (13) and (14). The auditor can determine the overall systems security risk and the corresponding reliability after having performed all the procedures. If the overall systems security risk achieved is not equal to or lower than an acceptable level, the assurance provider can either extend certain audit procedures to collect more evidence or issue a qualified opinion by mentioning the weaknesses in the system.

COMPARISON OF SYSTEMS SECURITY RISK FORMULA WITH THE NETWORK MODEL

In this section, we compare the two systems security risk models developed in this paper; one based on the exact network evidential diagram as given in Figure 1, and the other using the analytical formula based on a tree type evidential diagram as given in Figure 2, which is an approximation of the network diagram in Figure 1. We convert the network diagram in Figure 1 into a tree type diagram in Figure 2 by decomposing an item of evidence that pertains to two assertions or sub-assertions into two separate items of evidence keeping the original level of support for each assertion or sub-assertion and treating the two items of evidence as independent. This decomposition allows us to create a tree type diagram and hence to derive the analytical formula for the systems security risk as given in (13). In general, as argued below theoretically and also shown through the sensitivity analysis later, the analytical formula derived in this paper for a tree type diagram yields a lower belief that the system is secure, implying a higher plausibility that systems not security (since Pl(~s) = 1 – Bel(s)), i.e., a higher systems security risk than the corresponding values obtained for the network structure. Also, we find that the analytical formula for the tree structure yields a higher belief that the system is not secure than the value for the network structure in Figure 1. These results suggest that the analytical formulas based on the tree structure yield conservative estimates of the overall beliefs (a lower belief that the system is secure, a higher risk and a higher belief that the systems is not secure than the values obtained from the network model).

Also in this section, we identify conditions under which the analytical formula yields almost the same result as obtained from the network type diagram. For these conditions, the analytical formula serves as a good approximation of the exact network model. We also indentify the conditions under which the two models yield significantly different results and discuss the implications of these findings on practice. Next two sub-sections are devoted to understanding the impact of converting the network model to a tree model on the systems security risk.

Impact of Converting a Network Diagram into a Tree Diagram

Here we want to analyze the impact of converting a network diagram into a tree diagram on overall beliefs. To understand the impact conceptually, we consider a simple network where one assertion, say A, (with two values: 'a', and '~a', respectively, representing that the assertion is true and not true) is related to two sub-assertions, A1 and A2 (with values 'a1' and '~a1', and 'a2' and '~a2', respectively, representing that the corresponding sub-assertion is true and not true) through the 'and' relationship, implying that A is true if and only if A1 is true and A2 is true. We also assume that we have single item of evidence that pertains to both the sub-assertions with the following set of belief masses:

$$m_{12}(a1),\ m_{12}(\sim a1),\ \text{and}\ m_{12}(\{a1, \sim a1\}), \tag{20a}$$

$$m_{12}(a2),\ m_{12}(\sim a2),\ \text{and}\ m_{12}(\{a2, \sim a2\}). \qquad (20b)$$

The above belief masses are obtained from the single item of evidence pertaining to two sub-assertions. To propagate these m-values to assertion A using Shenoy and Shafer (1986) approach, we need to first express them in terms of belief masses on to the joint space of A1 and A2, Θ_{12} = {a1a2, a1~a2, ~a1a2, ~a1~a2}, and then propagate the resulting m-values through the 'and' relationship to assertion A. There are many possible values on the joint space that would yield the above belief masses in (20). We use Srivastava and Cogger algorithm (see Srivastava 1997) to obtain a belief mass distribution on the joint space that maintains the highest level of interdependencies in the two sets since they are coming from the same evidence. When these m-values are propagated through the 'and' node and marginalized to assertion A, we obtain the following set of m-values, beliefs and plausibilities at A:

$$m_N(a) = \min\{m_{12}(a1), m_{12}(a2)\}, \qquad (21a)$$

$$m_N(\sim a) = \max\{m_{12}(\sim a1), m_{12}(\sim a2)\}. \qquad (21b)$$

$$Bel_N(a) = \min\{m_{12}(a1), m_{12}(a2)\}, \qquad (21c)$$

$$Bel_N(\sim a) = \max\{m_{12}(\sim a1), m_{12}(\sim a2)\}. \qquad (21d)$$

$$Pl_N(\sim a) = 1 - \min\{m_{12}(a1), m_{12}(a2)\}, \qquad (21e)$$

The subscript N stands for network.

Now let us consider the situation where the above evidence is decomposed into two separate and independent items of evidence. Using Srivastava et al (1995) to propagate beliefs from the two sub-assertions to assertion A through the 'and' relationship, we obtain the following set of m-values, beliefs, and plausibilities at A:

$$m_T(a) = m_{12}(a1)m_{12}(a2), \qquad (22a)$$

$$m_T(\sim a) = m_{12}(\sim a1) + m_{12}(\sim a2) - m_{12}(\sim a1)m_{12}(\sim a2). \qquad (22b)$$

$$\mathrm{Bel}_T(a) = m_{12}(a1)m_{12}(a2), \tag{22c}$$

$$\mathrm{Bel}_T(\sim a) = m_{12}(\sim a1) + m_{12}(\sim a2) - m_{12}(\sim a1)m_{12}(\sim a2). \tag{22d}$$

$$\mathrm{Pl}_T(\sim a) = 1 - m_{12}(a1)m_{12}(a2). \tag{22e}$$

The subscript T above stands for tree.

As one can see from (21) and (22), the belief that the assertion A is true, Bel(a), is always lower for the tree model than for the network model (compare 21c with 22c). Also, the belief that assertion A is not true, Bel(~a), is always higher for the tree model than for the network model (compare 21d with 22d). Also, the risk that the assertion A is not true measured in terms of plausibility function is always higher for the tree model than for the network model (compare 21e with 22e). In other words, the tree model would always yield a higher risk than that of the network model.

The differences between the two sets of risks measured in terms of plausibility function that A is not true is given by the following equations:

$$\mathrm{Pl}_T(\sim a) - \mathrm{Pl}_N(\sim a) = \min\{m_{12}(a1), m_{12}(a2)\} - m_{12}(a1)m_{12}(a2) \geq 0. \tag{23}$$

Analyzing Equation (23), we find that the risk using the tree model is always greater than the risk using the network model. Also, the difference between these risks increases for $m_{12}(a1) = m_{12}(a2)$ as these m-values increase. The difference reaches a maximum value of 0.25 when $m_{12}(a1) = m_{12}(a2) = 0.5$, and reduces to a small value as the difference between the two m-values, $m_{12}(a1)$ and $m_{12}(a2)$, increases. The difference is zero if one of the m-values is zero. The above example shows that the risk measured in terms of plausibility function would always be higher for a tree model than for a network model if the sub-assertions are related to the main assertion through the ‘and’ relationship.

Sensitivity Analysis of Network Model versus Tree Model

Here we perform three different types of analyses to compare the overall systems security risk for the two models: network model and tree model. For the network model in Figure 1, we use the software "Auditor's Assistant" developed by Shafer et al. (1988) to compute the overall systems security risk. For the tree model we use the analytical formula derived in (13). We compute the systems security risk for the input beliefs given in Figure 1 and Figure 2. Note that all these input values are in support of the assertions or sub-assertions implying that, in the present case, all these items of evidence are positive. Figure 4 plots the overall systems security risk for the two models as a function of the increase and decrease in the input beliefs for all the items of evidence in Figure 1 and Figure 2.

We can see from Figure 4 that the difference between the two values of the systems security risk is not significant. The highest difference is at the lower end and the lowest difference is at the higher end. This result implies that a network model can be replaced by a tree model without any significant impact on the overall security risk and, thus, one can use the analytical formula developed in (13) for the tree model for assessing security risk, especially if m-values for the negation of the variables are zero, which will be the situation in the planning stage of an audit. The auditor, when planning the audit, would not have negative items of evidence pertaining to the assertions or sub-assertions of interest.

In the above discussion, we assumed that the evidence pertaining to more than one variable provides the same level of support to all the associated variables. As the second scenario, we consider the situation where one piece of evidence provides different levels of support to different variables. Figure 5 illustrates the results of this analysis: that the evidence pertaining to two variables provides different levels of support to the two variables. We start with an input of 0.5 level of support for both variables. Then, we increase the support by 10, 20, 30, 40, 50 and 60 percent for one variable, and decrease the support by 10, 20, 30, 40, 50 and 60 percent for the other variable. The largest difference of the resulting overall belief between the network model and the tree model is only 0.011 when the inputs in both cases are the same for the two variables.

The first two scenarios dealt with only positive items of evidence. Next, we consider the third scenario where the two models use negative evidence. We input 0.2, 0.1, 0, -0.1, -0.2, -0.3, -0.4 and -0.5 as the strength of evidence for those items of evidence that pertain to two variables. The five negative values given above imply that the items of evidence provide support to the negation of the corresponding variable. Figure 6 presents a plot of the overall systems security risk as a function of the changes in the input beliefs obtained from the evidence that pertain to two variables. The difference between the network model and the tree model is the highest for strong negative input beliefs. However, this difference decrease as the strength of the negative evidence decreases. In fact, the two models yield identical values when these items of evidence (pertaining to two variables) have no input beliefs. This result is logical because in such a situation the network reduces to a tree yielding exactly the same value.

One can also see that the overall systems security risk for the tree model, in the cases considered, is always higher than the systems security risk for the network model. This result implies that the analytical formula based on the tree model is more conservative than the value obtained from the network model. Also, we see that the analytical formula based on the tree model is a good approximation of the network model when the items of evidence are either positive or mixed evidence with very week negative strength. The analytical formula is not a good approximation of network model if we have strong negative piece of evidence. However, in such a situation, it would not make sense for the auditor to determine the overall belief whether the systems is secure or not; he/she already has the knowledge that the system is not secure based on the negative evidence and thus would like to fix the problem rather trying to aggregate the evidence.

SUMMARY AND CONCLUSIONS

In this paper we have developed general formulas for systems security risk and systems reliability under Dempster-Shafer theory of belief functions for planning and evaluation of systems reliability for SysTrust services. To derive the analytical formula, we had to convert the evidential diagram that was a network into a tree because deriving analytical formula for a network can become very complex. Our formulas are valid for positive, negative, and mixed items of evidence. We compared the assessments of the systems security risk based on the analytical formula with the values obtained for the corresponding network model and found that the analytical formula is a good substitute for the network model under certain realistic conditions. Realistic conditions means that 1) we assume positive evidence, especially in planning phase (Srivastava and Shafer 1992), 2) under mixed evidence, we have very weak negative support, and 3) under strong negative support, the auditor would not need the model rather would fix the problem. Thus, using the analytical formula eliminates the computational complexities of propagating beliefs in a network (Srivastava 1995), and allows assurance providers to use a simple spreadsheet to combine all the evidence. Our results also show that the analytical formula based on tree structure is more conservative than the network model. This is because treating one item of evidence in a network, which provides, say, 0.8 level of support jointly to two sub-assertions, would become 0.64 (= 0.8x0.8) level of support to both sub-assertions if the evidence were split into two separate items of evidence, each pertaining to individual sub-assertions and thus yielding a higher risk (0.36 for the above example) than in the case when the evidence was not split (a risk of 0.2).

Of course, like many other studies, this study has limitations too. One limitation is that our risk and reliability formulas are based on a tree type structure which is an approximation of the exact network diagram. Under this approximation, we assume that a single item of evidence in the network which pertains to several assertions or sub-assertions is split into several independent items of evidence each pertaining to individual assertion or sub-assertion. Another limitation is that all our input beliefs used in the analysis are hypothetical numbers. It would be interesting to use inputs from the experts who perform such engagements.

There are several research opportunities in this area. First, it would be important to investigate whether auditors' uncertainty judgments can be mapped using DS theory. Second, it would be interesting to apply the formulas in an actual assurance engagement and assess the advantages and disadvantages of such formulas. Third, how should we measure the strength of evidence under belief functions? Should we use numerical scale or mnemonic scale? How should a mnemonic scale be calibrated?

REFERENCE

Akresh, A. D., J. K. Loebbecke and W. R. Scott. 1988. Audit Approaches and Techniques. In *Research Opportunities in Auditing: The Second Decade*, edited by A. R. Abdel-khalik and Ira Solomon, Sarasota, FL: AAA, 13-55.

American Institute of Certified Public Accountants (AICPA). 2006. *SAS 107: Audit Risk and Materiality in Conducting an Audit*. American Institute of Certified Public Accountants, New York.

__________. 2003. *AICPA/CICA Suitable Trust Services Criteria and Illustrations*. American Institute of Certified Public Accountants, New York.

__________. 1983. *SAS No. 47: Audit Risk and Materiality in Conducting an Audit*. American Institute of Certified Public Accountants, New York.

Brodkin, J. 2007. IT spending to surpass $3 trillion. *Network World*. October 8.

Boritz, J. E, D. McPhie, and B. Walker. 2000. In systems we trust. *CA Magazine* 133 (2): 47-49.

Bovee, M., R. P. Srivastava and B. Mak. 2003. A conceptual framework and belief-function approach to assessing overall information quality. *International Journal of Intelligent Systems* 18 (1): 51-74.

Curley, S. P., and J. I. Golden. 1994. Using belief functions to represent degrees of belief. *Organizational Behavior and Human Decision Processes* 58: 271-303.

Doyle, J., W. Ge and S. McVay. 2007. Accruals Quality and Internal Control over Financial Reporting. *The Accounting Review*, 82 (5):1141-1170.

Ettredge, M., J. Heintz, C. Li and S. Scholz. 2007. Auditor Realignments Accompanying Implementation of SOX 404 Reporting Requirements. Working Paper, University of Kansas.

Gordon, J., and E. H. Shortliffe. 1990. The Dempster-Shafer Theory of Evidence. In Readings in Uncertain Reasoning edited by G. Shafer and J. Pearl. San Mateo, California: Morgan Kaufmann Publishers, Inc, California.

Harrison, K., R. P. Srivastava, and R. D. Plumlee. 2002. Auditors' evaluations of uncertain audit evidence: belief functions versus probabilities. In Belief Functions in Business Decisions, edited by R. P. Srivastava and T. Mock, Physica-Verlag, Heidelberg, Springer-Verlag Company: 161-183.

Mock, T.J., A. Wright and R. P. Srivastava. 1998. Audit program planning using a belief function framework. Proceedings of the 1998 Deloitte & Touche University of Kansas Symposium on Auditing Problems. 66-85.

Public Company Accounting Oversight Board (PCAOB). 2004. *Auditing Standard No. 2— An audit of internal control over financial reporting performed in conjunction with an audit of financial statements*. Public Company Accounting Oversight Board.

Scott, J. E. 1999. The FoxMeyer Drugs' Bankruptcy: Was it a Failure of ERP? *Proceedings of the Americas Conference on Information Systems*. Milwaukee, WI, USA, August 13-15: 223-225.

Shafer, G. 1976. *A Mathematical Theory of Evidence.* Princeton, N.J. Princeton University Press.

Shafer, G., P. P. Shenoy, and R. P. Srivastava. 1988. Auditor's Assistant: a knowledge engineering tool for audit decisions. *Proceedings of the 1988 Touche Ross University of Kansas Symposium on Auditing Problems*: 61-79.

Shafer, G. and R. P. Srivastava. 1990. The Bayesian and belief-function formalisms: a general perspective for auditing. *Auditing: A Journal of Practice and Theory* (Supplement): 110-148.

Shenoy, P. P. and G. Shafer, "Propagating Belief Functions with Local Propagation," *IEEE Expert*, Vol. 1 (1986) pp. 43-52.

Shenoy, C. and P. P. Shenoy. 2002. Modeling financial portfolios using belief functions. In Belief Functions in Business Decisions, edited by R. P. Srivastava and T. Mock, Physica-Verlag, Heidelberg, Springer-Verlag Company: 316-322.

Srivastava, R. P. 1995. The belief-function approach to aggregating audit evidence. *Internal Journal of Intelligent Systems* (March): 329-356.

Srivastava, R. P. 1997. Audit Decisions Using Belief Functions: A Review," *Control and Cybernetics*, Vol. 26, No.2: 135-160.

Srivastava, R. P. 2005. Alternative form of Dempster's Rule for binary variables. *International Journal of Intelligent Systems* 20 (8): 789-797.

Srivastava, R.P., M. Buche, and T. Roberts. 2005. Belief Function Approach to Evidential Reasoning in Causal Maps. In *Causal Mapping for Information Systems and Technology Research: Approaches, Advances and Illustrations*, edited by V. K. Narayanan and D. Armstrong, Idea Group, Inc., Hersey: pp. 109-141.

Srivastava, R. P. and D. Datta. 2002. Evaluating mergers and acquisitions: a belief function approach. In *Belief Functions in Business Decisions*, edited by R. P. Srivastava and T. Mock, Physica-Verlag, Heidelberg, Springer-Verlag Company: 222-251.

Srivastava, R. P., S. Dutta, and R. Johns. 1996. An expert system approach to audit planning and evaluation in the belief-function framework. *International Journal of Intelligent Systems in Accounting, Finance and Management* 5: 165-183.

Srivastava, R. P. and H. Lu 2002. Structural analysis of audit evidence using belief functions. *Fuzzy Sets and Systems* 131 (1): 107-120.

Srivastava, R. P., and T. Mock. 2002. *Belief Functions in Business Decisions*. Physica-Verlag, Springer-Verlag Company, Heidelberg.

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

Srivastava, R. P., T. Mock, and J. Turner. 2007. Analytical Formulas for Risk Assessment for a Class of Problems where Risk Depends on Three Interrelated Variables. *International Journal of Approximate Reasoning* 45: 123–151.

Srivastava, R. P. and G. Shafer. 1992. Belief–function formulas for audit risk. *The Accounting Review* 67 (2): 249-283.

Srivastava, R. P., P. Shenoy and G. Shafer. 1995. Propagating beliefs in an ‘AND’ tree. *International Journal of Intelligent Systems* 10: 647-664.

Sun, L., R. P. Srivastava**,** and T. Mock. 2006. An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions. *Journal of Management Information Systems* 22 (4): 109-142.

Table 1: Principles, Sub-Principle, and Sub-Sub-Principles for System Security in Trust Services

Principle	Sub-Principle	Sub-Sub Principle
1. Security (S)	1.1. Protection against unauthorized logical access (L)	1.1.1. Policies exist to ensure systems are protected against unauthorized logical access (LP).
		1.1.2. System security policies pertaining to logical access are communicated to authorized users (LC).
		1.1.3. Procedures exist to protect against unauthorized logical access (LR).
	1.2. Protection against unauthorized physical access (P)	1.2.1. Policies exist to ensure systems are protected against unauthorized physical access (PP).
		1.2.2. System security policies pertaining to physical access are communicated to authorized users (PC).
		1.2.3. Procedures exist to protect against unauthorized physical access (PR).
	1.3. Protection against infection by computer viruses (V)	1.3.1. Policies exist to ensure systems are protected against virus infection (VP).
		1.3.2. System security policies pertaining to virus infection are communicated to authorized users (VC).
		1.3.3. Procedures exist to protect against virus infection (VR).

Table 2: List of Symbols and Their Descriptions

Symbol	**Descriptions of the variable**
S {*s*, ~*s*}	S represents the assertion 'System is **secure**, i.e., the system is protected against unauthorized access'. Its two values, *s*, and ~*s*, respectively, represent the value that the variable S is true and is not true.
L {*l*, ~*l*}	L represents the assertion 'System is protected against unauthorized **logical** access'. Its two values, *l*, and ~*l*, respectively, represent the value that the variable L is true and is not true.
P {*p*, ~*p*}	P represents the assertion 'System is protected against unauthorized **physical** access'. Its two values, *p*, and ~*p*, respectively, represent the value that the variable P is true and is not true.
V (*v*, ~*v*}	V represents the assertion 'Systems is protected against infection by computer **viruses'.** Its two values, *v*, and ~*v*, respectively, represent the value that the variable V is true and is not true.
LP {*lp*, ~*lp*}	LP represents the assertion '**Policies** exist to ensure that the system is protected against unauthorized **logical** access.' Its two values, *lp* and ~*lp*, respectively, represent the values that the variable, LP, is true and is not true.
LC {*lc*, ~*lc*}	LC represents the assertion 'Security policies pertaining to **logical** access are **communicated** to users.' Its two values, *lc* and ~*lc*, respectively, represent the value that the variable, LC, is true and is not true.
LR {*lr*, ~*lr*}	LR represents the assertion **'Procedure** exists to protect against unauthorized **logical** access.' Its two values, *lr* and ~*lr*, respectively, represent the value that the variable, LR, is true and is not true.
PP {*pp*, ~*pp*}	PP represents the assertion '**Policies** exist to ensure that the system is protected against unauthorized **physical** access.' Its two values, *pp* and ~*pp*, respectively, represent the value that the variable, PP, is true and is not true.
PC {*pc*, ~*pc*}	PC represents the assertion 'Security policies pertaining to **physical** access are **communicated** to users.' Its two values, *pc* and ~*pc*, respectively, represent the value that the variable, PC, is true and is not true.
PR {*pr*, ~*pr*}	PR represents the assertion **'Procedure** exists to protect the system against unauthorized **physical** access.' Its two values, *pr* and ~*pr*, respectively, represent the value that the variable, PR, is true and is not true.
VP {*vp*, ~*vp*}	VP represents the assertion **'Policies** exist to ensure the system is protected against computer **viruses.'** Its two values, *vp* and ~*vp*, respectively, represent the value that the variable, VP, is true and is not true.
VC {*vc*, ~*vc*}	VC represents the assertion 'Security policies pertaining to **virus** infection are **communicated** to users.' Its two values, *vc* and ~*vc*, respectively, represent the value that the variable, VC, is true and is not true.
VR {*vr*, ~*vr*}	VR represents the assertion **'Procedure** exists to protect the system against computer **viruses.'** Its two values, *vr* and ~*vr*, respectively, represent the value that the variable, VR, is true and is not true.
m..(..)	Basic belief mass (m-value) for the value of the variable in the parenthesis from the evidence represented by the subscript
$m_{S \leftarrow L,P,V}$	The basic belief mass (m-value) on variable 'S' from all the variables L, P, V.

Table 3. The belief mass function at each variable after combining all the evidence at each variable in Figure 3

Variable	The belief mass function as a result of combining all the independent items of evidence pertaining to the variable using the Srivastava approach (2005)	Variable	The belief mass function as a result of combining all the independent items of evidence pertaining to the variable using the Srivastava approach (2005)
LP	$m_{LP}(lp) = 1-\prod_{i=1}^{q_{LP}}(1-m_i(lp))/K_{LP}$	PP	$m_{PP}(pp) = 1-\prod_{i=1}^{q_{PP}}(1-m_i(pp))/K_{PP}$
	$m_{LP}(\sim lp) = 1-\prod_{i=1}^{q_{LP}}(1-m_i(\sim lp))/K_{LP}$		$m_{PP}(\sim pp) = 1-\prod_{i=1}^{q_{PP}}(1-m_i(\sim pp))/K_{PP}$
	$m_{LP}(\{lp,\sim lp\}) = \prod_{i=1}^{q_{LP}} m_i(\{lp,\sim lp\})/K_{LP}$		$m_{PP}(\{pp,\sim pp\}) = \prod_{i=1}^{q_{PP}} m_i(\{pp,\sim pp\})/K_{PP}$
	$K_{LP} = \prod_{i=1}^{q_{LP}}(1-m_i(lp))+\prod_{i=1}^{q_{LP}}(1-m_i(\sim lp))-\prod_{i=1}^{q_{LP}} m_i(\{lp,\sim lp\})$		$K_{PP} = \prod_{i=1}^{q_{PP}}(1-m_i(pp))+\prod_{i=1}^{q_{PP}}(1-m_i(\sim pp))-\prod_{i=1}^{q_{PP}} m_i(\{pp,\sim pp\})$
LC	$m_{LC}(lc) = 1-\prod_{i=1}^{q_{LC}}(1-m_i(lc))/K_{LC}$	PC	$m_{PC}(pc) = 1-\prod_{i=1}^{q_{PC}}(1-m_i(pc))/K_{PC}$
	$m_{LC}(\sim lc) = 1-\prod_{i=1}^{q_{LC}}(1-m_i(\sim lc))/K_{LC}$		$m_{PC}(\sim pc) = 1-\prod_{i=1}^{q_{PC}}(1-m_i(\sim pc))/K_{PC}$
	$m_{LC}(\{lc,\sim lc\}) = \prod_{i=1}^{q_{LC}} m_i(\{lc,\sim lc\})/K_{LC}$		$m_{PC}(\{pc,\sim pc\}) = \prod_{i=1}^{q_{PC}} m_i(\{pc,\sim pc\})/K_{PC}$
	$K_{LC} = \prod_{i=1}^{q_{LC}}(1-m_i(lc))+\prod_{i=1}^{q_{LC}}(1-m_i(\sim lc))-\prod_{i=1}^{q_{LC}} m_i(\{lc,\sim lc\})$		$K_{PC} = \prod_{i=1}^{q_{PC}}(1-m_i(pc))+\prod_{i=1}^{q_{PC}}(1-m_i(\sim pc))-\prod_{i=1}^{q_{PC}} m_i(\{pc,\sim pc\})$
LR	$m_{LR}(lr) = 1-\prod_{i=1}^{q_{LR}}(1-m_i(lr))/K_{LR}$	PR	$m_{PR}(pr) = 1-\prod_{i=1}^{q_{PR}}(1-m_i(pr))/K_{PR}$
	$m_{LR}(\sim lr) = 1-\prod_{i=1}^{q_{LR}}(1-m_i(\sim lr))/K_{LR}$		$m_{PR}(\sim pr) = 1-\prod_{i=1}^{q_{PR}}(1-m_i(\sim pr))/K_{PR}$
	$m_{LR}(\{lr,\sim lr\}) = \prod_{i=1}^{q_{LR}} m_i(\{lr,\sim lr\})/K_{LR}$		$m_{PR}(\{pr,\sim pr\}) = \prod_{i=1}^{q_{PR}} m_i(\{pr,\sim pr\})/K_{PR}$
	$K_{LR} = \prod_{i=1}^{q_{LR}}(1-m_i(lr))+\prod_{i=1}^{q_{LR}}(1-m_i(\sim lr))-\prod_{i=1}^{q_{LP}} m_i(\{lr,\sim lr\})$		$K_{PR} = \prod_{i=1}^{q_{PR}}(1-m_i(pr))+\prod_{i=1}^{q_{PR}}(1-m_i(\sim pr))-\prod_{i=1}^{q_{PR}} m_i(\{pr,\sim pr\})$

Table 3 (Continued). The belief mass function at each variable after combining all the evidence at each variable

Variable	The belief mass function as a result of combining all the independent items of evidence pertaining to the variable using the Srivastava approach (2005)	Variable	The belief mass function as a result of combining all the independent items of evidence pertaining to the variable using the Srivastava approach (2005)
VP	$\mathrm{m}_{\mathrm{VP}}(vp) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{VP}}}(1-\mathrm{m_i}(vp))/\mathrm{K_{VP}}$	L	$\mathrm{m}_{\mathrm{L}}(l) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{L}}}(1-\mathrm{m_i}(l))/\mathrm{K_{L}}$
	$\mathrm{m}_{\mathrm{VP}}(\sim vp) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{VP}}}(1-\mathrm{m_i}(\sim vp))/\mathrm{K_{VP}}$		$\mathrm{m}_{\mathrm{L}}(\sim l) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{L}}}(1-\mathrm{m_i}(\sim l))/\mathrm{K_{L}}$
	$\mathrm{m}_{\mathrm{VP}}(\{vp,\sim vp\}) = \prod_{\mathrm{i=1}}^{\mathrm{q_{VP}}}\mathrm{m_i}(\{vp,\sim vp\})/\mathrm{K_{VP}}$		$\mathrm{m}_{\mathrm{L}}(\{l,\sim l\}) = \prod_{\mathrm{i=1}}^{\mathrm{q_{L}}}\mathrm{m_i}(\{l,\sim l\})/\mathrm{K_{L}}$
	$\mathrm{K_{VP}} = \prod_{\mathrm{i=1}}^{\mathrm{q_{VP}}}(1-\mathrm{m_i}(vp)) + \prod_{\mathrm{i=1}}^{\mathrm{q_{VP}}}(1-\mathrm{m_i}(\sim vp)) - \prod_{\mathrm{i=1}}^{\mathrm{q_{VP}}}\mathrm{m_i}(\{vp,\sim vp\})$		$\mathrm{K_{L}} = \prod_{\mathrm{i=1}}^{\mathrm{q_{L}}}(1-\mathrm{m_i}(l)) + \prod_{\mathrm{i=1}}^{\mathrm{q_{L}}}(1-\mathrm{m_i}(\sim l)) - \prod_{\mathrm{i=1}}^{\mathrm{q_{L}}}\mathrm{m_i}(\{l,\sim l\})$
VC	$\mathrm{m}_{\mathrm{VC}}(vc) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{VC}}}(1-\mathrm{m_i}(vc))/\mathrm{K_{VC}}$	P	$\mathrm{m}_{\mathrm{P}}(p) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{P}}}(1-\mathrm{m_i}(p))/\mathrm{K_{P}}$
	$\mathrm{m}_{\mathrm{VC}}(\sim vc) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{VC}}}(1-\mathrm{m_i}(\sim vc))/\mathrm{K_{VC}}$		$\mathrm{m}_{\mathrm{P}}(\sim p) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{P}}}(1-\mathrm{m_i}(\sim p))/\mathrm{K_{P}}$
	$\mathrm{m}_{\mathrm{VC}}(\{vc,\sim vc\}) = \prod_{\mathrm{i=1}}^{\mathrm{q_{VC}}}\mathrm{m_i}(\{vc,\sim vc\})/\mathrm{K_{VC}}$		$\mathrm{m}_{\mathrm{P}}(\{p,\sim p\}) = \prod_{\mathrm{i=1}}^{\mathrm{q_{P}}}\mathrm{m_i}(\{p,\sim p\})/\mathrm{K_{P}}$
	$\mathrm{K_{VC}} = \prod_{\mathrm{i=1}}^{\mathrm{q_{VC}}}(1-\mathrm{m_i}(vc)) + \prod_{\mathrm{i=1}}^{\mathrm{q_{VC}}}(1-\mathrm{m_i}(\sim vc)) - \prod_{\mathrm{i=1}}^{\mathrm{q_{VC}}}\mathrm{m_i}(\{vc,\sim vc\})$		$\mathrm{K_{P}} = \prod_{\mathrm{i=1}}^{\mathrm{q_{P}}}(1-\mathrm{m_i}(p)) + \prod_{\mathrm{i=1}}^{\mathrm{q_{P}}}(1-\mathrm{m_i}(\sim p)) - \prod_{\mathrm{i=1}}^{\mathrm{qP}}\mathrm{m_i}(\{p,\sim p\})$
VR	$\mathrm{m}_{\mathrm{VR}}(vr) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{VR}}}(1-\mathrm{m_i}(vr))/\mathrm{K_{VR}}$	V	$\mathrm{m}_{\mathrm{V}}(v) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{V}}}(1-\mathrm{m_i}(v))/\mathrm{K_{V}}$
	$\mathrm{m}_{\mathrm{VR}}(\sim vr) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{VR}}}(1-\mathrm{m_i}(\sim vr))/\mathrm{K_{VR}}$		$\mathrm{m}_{\mathrm{V}}(\sim v) = 1-\prod_{\mathrm{i=1}}^{\mathrm{q_{V}}}(1-\mathrm{m_i}(\sim v))/\mathrm{K_{V}}$
	$\mathrm{m}_{\mathrm{VR}}(\{vr,\sim vr\}) = \prod_{\mathrm{i=1}}^{\mathrm{q_{VR}}}\mathrm{m_i}(\{vr,\sim vr\})/\mathrm{K_{VR}}$		$\mathrm{m}_{\mathrm{V}}(\{v,\sim v\}) = \prod_{\mathrm{i=1}}^{\mathrm{q_{V}}}\mathrm{m_i}(\{v,\sim v\})/\mathrm{K_{V}}$
	$\mathrm{K_{VR}} = \prod_{\mathrm{i=1}}^{\mathrm{q_{VR}}}(1-\mathrm{m_i}(vr)) + \prod_{\mathrm{i=1}}^{\mathrm{q_{VR}}}(1-\mathrm{m_i}(\sim vr)) - \prod_{\mathrm{i=1}}^{\mathrm{q_{VR}}}\mathrm{m_i}(\{vr,\sim vr\})$		$\mathrm{K_{V}} = \prod_{\mathrm{i=1}}^{\mathrm{q_{V}}}(1-\mathrm{m_i}(v)) + \prod_{\mathrm{i=1}}^{\mathrm{q_{V}}}(1-\mathrm{m_i}(\sim v)) - \prod_{\mathrm{i=1}}^{\mathrm{q_{V}}}\mathrm{m_i}(\{v,\sim v\})$

Table 4: The belief masses at variables L, P, and V, propagated from the corresponding sub-sub-principles and the belief masses at sub-sub-principle with more than one item of evidence for Figure 2.

Sub-Principle and Sub-Sub-Principle	**The belief mass propagated from the corresponding sub-sub-principles and the belief masses at the sub-sub-principles**
L	$m_{L\leftarrow LP,LC,LR}(l) = m_{LP}(lp)m_{LC}(lc)m_{LR}(lr)$
	$m_{L\leftarrow LP,LC,LR}(\sim l) = 1- [1-m_{LP}(\sim lp)][1-m_{LC}(\sim lc)][1-m_{LR}(\sim lr)]$
P	$m_{P\leftarrow PP,PC,PR}(p) = m_{PP}(pp)m_{PC}(pc)m_{PR}(pr)$
	$m_{P\leftarrow PP,PC,PR}(\sim p) = 1- [1-m_{PP}(\sim pp)][1-m_{PC}(\sim pc)][1-m_{PR}(\sim pr)]$
V	$m_{V\leftarrow VP,VC,VR}(v) = m_{VP}(vp)m_{VC}(vc)m_{VR}(vr)$
	$m_{V\leftarrow VP,VC,VR}(\sim v) = 1- [1-m_{VP}(\sim vp)][1-m_{VC}(\sim vc)][1-m_{VR}(\sim vr)]$
LP	$m_{LP}(lp) = 1 - [1-m_{LP1}(lp)][1-m_{LP2}(lp)]/K_{LP}$
	$m_{LP}(\sim lp) = 1 - [1-m_{LP1}(\sim lp)][1-m_{LP2}(\sim lp)]/K_{LP}$
	$m_{LP}(\{lp, \sim lp\}) = m_{LP1}(\{lp, \sim lp\})m_{LP2}(\{lp, \sim lp\})/K_{LP}$
	$K_{LP} = [1-m_{LP1}(lp)][1-m_{LP2}(lp)] + [1-m_{LP1}(\sim lp)][1-m_{LP2}(\sim lp)] - m_{LP1}(\{lp, \sim lp\})m_{LP2}(\{lp, \sim lp\})$
PR	$m_{PR}(pr) = 1 - [1-m_{PR1}(pr)][1-m_{PR2}(pr)]/K_{PR}$
	$m_{PR}(\sim pr) = 1 - [1-m_{PR1}(\sim pr)][1-m_{PR2}(\sim pr)]/K_{PR}$
	$m_{PR}(\{pr, \sim pr\}) = m_{PR1}(\{pr, \sim pr\})m_{PR2}(\{pr, \sim pr\})/K_{PR}$
	$K_{PR} = [1-m_{PR1}(pr)][1-m_{PR2}(pr)] + [1-m_{PR1}(\sim pr)][1-m_{PR2}(\sim pr)] - m_{PR1}(\{pr, \sim pr\})m_{PR2}(\{pr, \sim pr\})$
VP	$m_{VP}(vp) = 1 - [1-m_{VP1}(vp)][1-m_{VP2}(vp)]/K_{VP}$
	$m_{VP}(\sim vp) = 1 - [1-m_{VP1}(\sim vp)][1-m_{VP2}(\sim vp)]/K_{VP}$
	$m_{VP}(\{vp, \sim vp\}) = m_{VP1}(\{vp, \sim vp\})m_{VP2}(\{vp, \sim vp\})/K_{VP}$
	$K_{VP} = [1-m_{VP1}(vp)][1-m_{VP2}(vp)] + [1-m_{VP1}(\sim vp)][1-m_{VP2}(\sim vp)] - m_{VP1}(\{vp, \sim vp\})m_{VP2}(\{vp, \sim vp\})$
VR	$m_{VR}(vr) = 1 - [1 - m_{VR1}(vr)][1 - m_{VR2}(vr)]/K_{VR}$
	$m_{VR}(\sim vr) = 1 - [1 - m_{VR1}(\sim vr)][1 - m_{VR2}(\sim vr)]/K_{VR}$
	$m_{VR}(\{vr, \sim vr\}) = m_{VR1}(\{vr, \sim vr\})m_{VR2}(\{vr, \sim vr\})/K_{VR}$
	$K_{VR} = [1 - m_{VR1}(vr)][1 - m_{VR2}(vr)] + [1 - m_{VR1}(\sim vr)][1 - m_{VR2}(\sim vr)] - m_{VR1}(\{vr, \sim vr\})m_{VR2}(\{vr, \sim vr\})$

Figure 1. Evidential Network for "System Security" Assurance

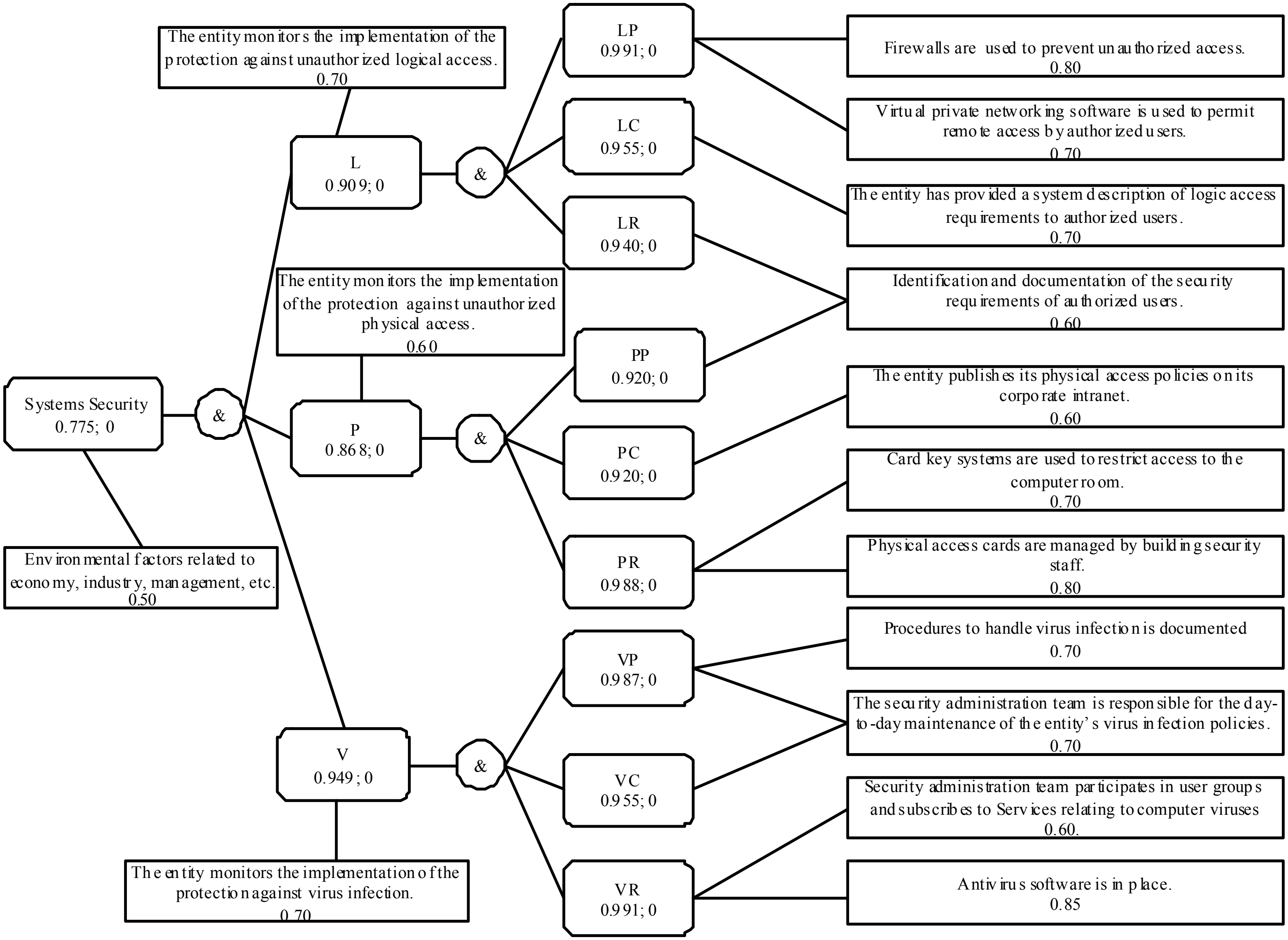
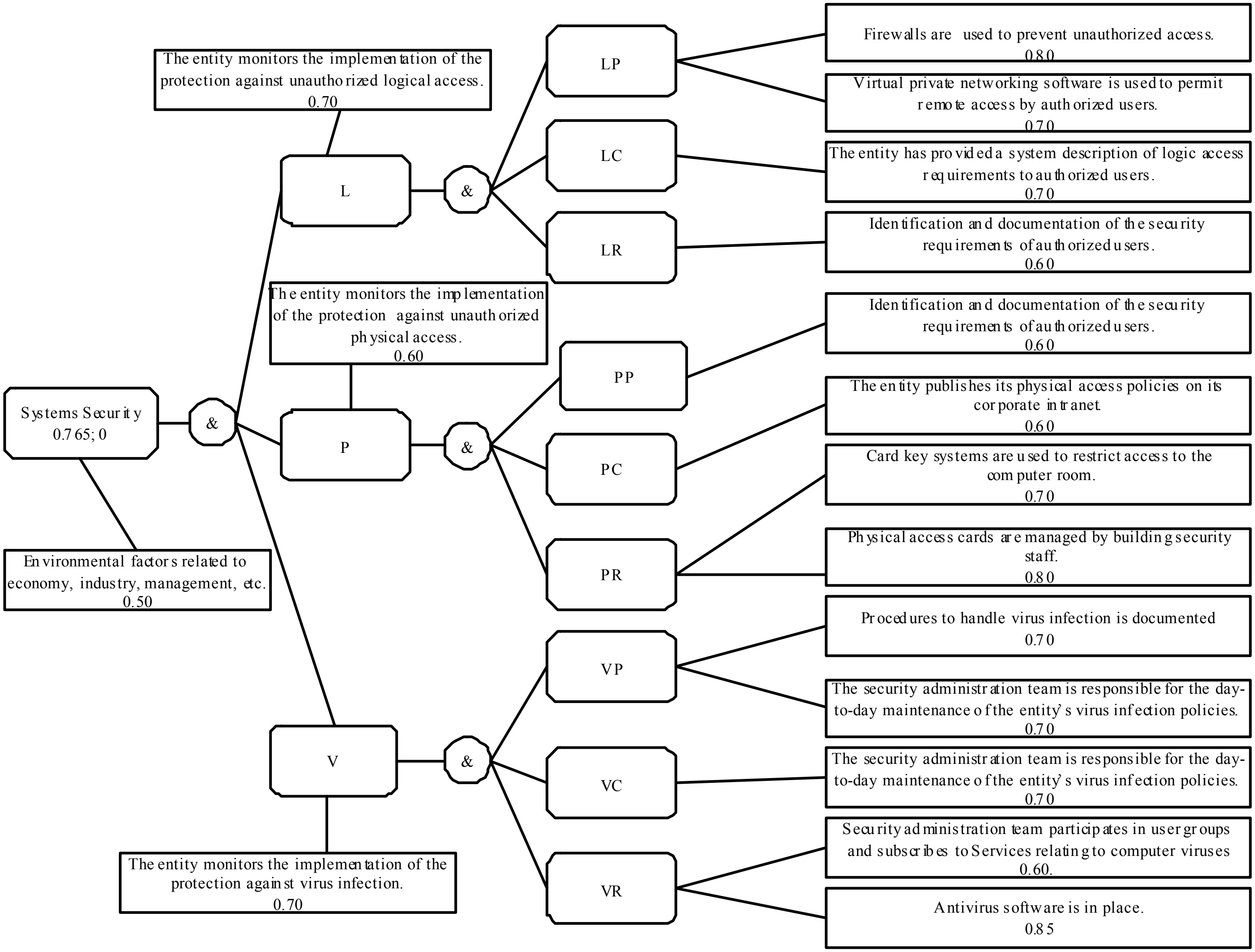

The entity monitors the implementation of the protection against unauthorized logical access. 0.70
L 0.909; 0
&
LP 0.991; 0
LC 0.955; 0
LR 0.940; 0
Firewalls are used to prevent unauthorized access. 0.80
Virtual private networking software is used to permit remote access by authorized users. 0.70
The entity has provided a system description of logic access requirements to authorized users. 0.70
Identification and documentation of the security requirements of authorized users. 0.60
The entity monitors the implementation of the protection against unauthorized physical access. 0.60
Systems Security 0.775; 0
&
P 0.868; 0
&
PP 0.920; 0
PC 0.920; 0
PR 0.988; 0
The entity publishes its physical access policies on its corporate intranet. 0.60
Card key systems are used to restrict access to the computer room. 0.70
Physical access cards are managed by building security staff. 0.80
Environmental factors related to economy, industry, management, etc. 0.50
V 0.949; 0
&
VP 0.987; 0
VC 0.955; 0
VR 0.991; 0
Procedures to handle virus infection is documented 0.70
The security administration team is responsible for the day-to-day maintenance of the entity's virus infection policies. 0.70
Security administration team participates in user groups and subscribes to Services relating to computer viruses 0.60.
Antivirus software is in place. 0.85
The entity monitors the implementation of the protection against virus infection. 0.70

Figure 2. Tree Diagram for “System Security” Assurance



Environmental factors related to economy, industry, management, etc. 0.50

The entity monitors the implementation of the protection against unauthorized logical access. 0.70

The entity monitors the implementation of the protection against unauthorized physical access. 0.60

The entity monitors the implementation of the protection against virus infection. 0.70

Firewalls are used to prevent unauthorized access. 0.80

Virtual private networking software is used to permit remote access by authorized users. 0.70

The entity has provided a system description of logic access requirements to authorized users. 0.70

Identification and documentation of the security requirements of authorized users. 0.60

Identification and documentation of the security requirements of authorized users. 0.60

The entity publishes its physical access policies on its corporate intranet. 0.60

Card key systems are used to restrict access to the computer room. 0.70

Physical access cards are managed by building security staff. 0.80

Procedures to handle virus infection is documented 0.70

The security administration team is responsible for the day-to-day maintenance of the entity's virus infection policies. 0.70

The security administration team is responsible for the day-to-day maintenance of the entity's virus infection policies. 0.70

Security administration team participates in user groups and subscribes to Services relating to computer viruses 0.60.

Antivirus software is in place. 0.85

Figure 3. A General Evidential Tree Diagram for "System Security" Assurance

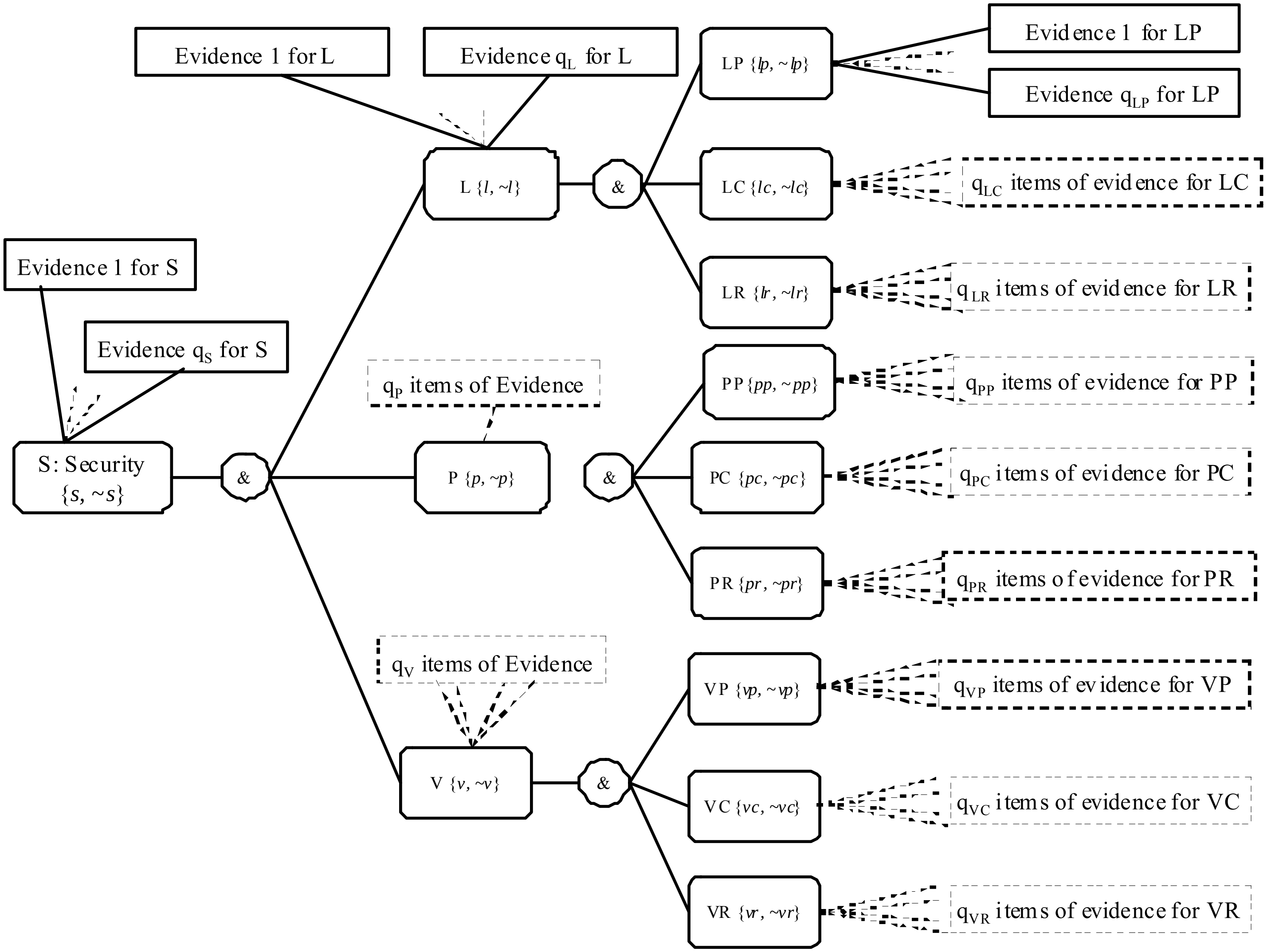


Figure 4. The impact of changes in the strength of evidence on the overall systems security risk that the system is not protected against unauthorized access.

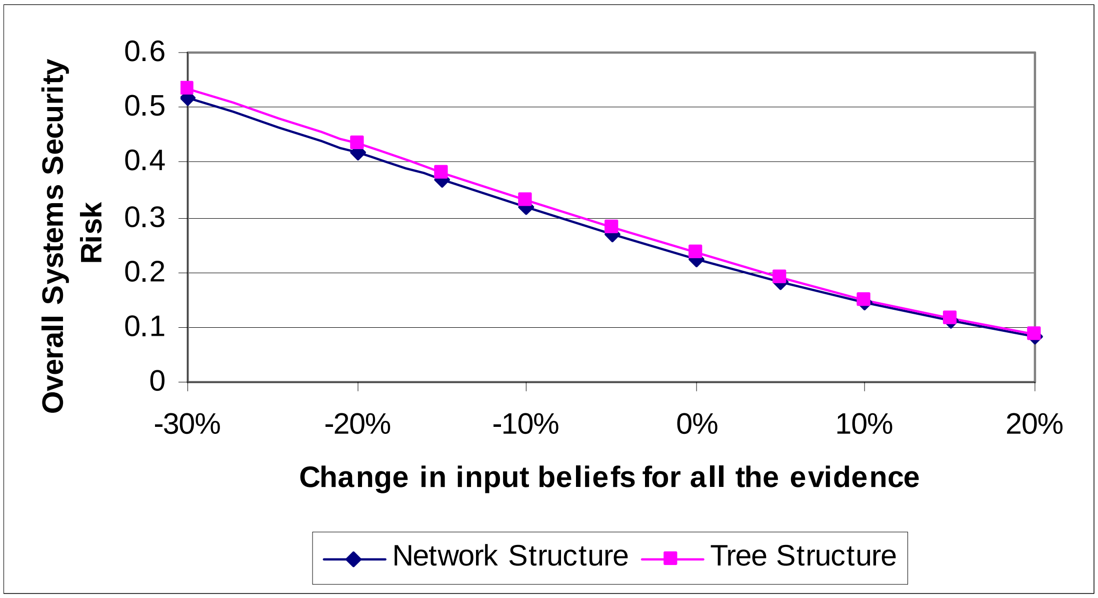


Figure 5. The impact of the change of the strength of evidence that pertains to more than one variable on the overall systems security risk that the system is not protected against unauthorized access.

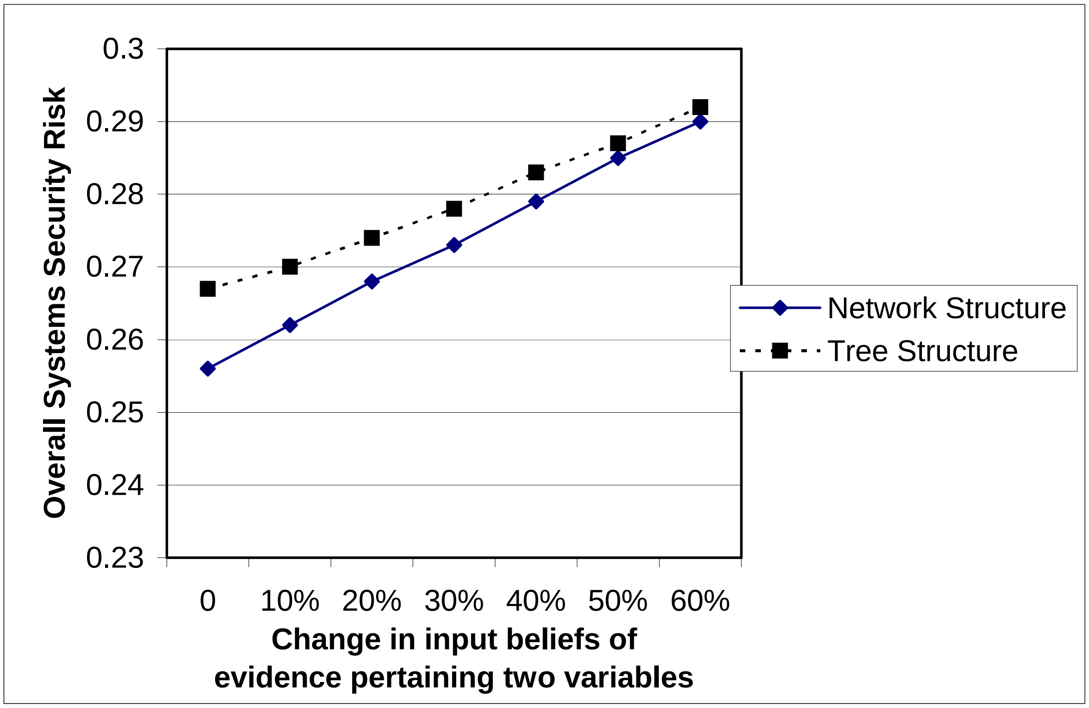
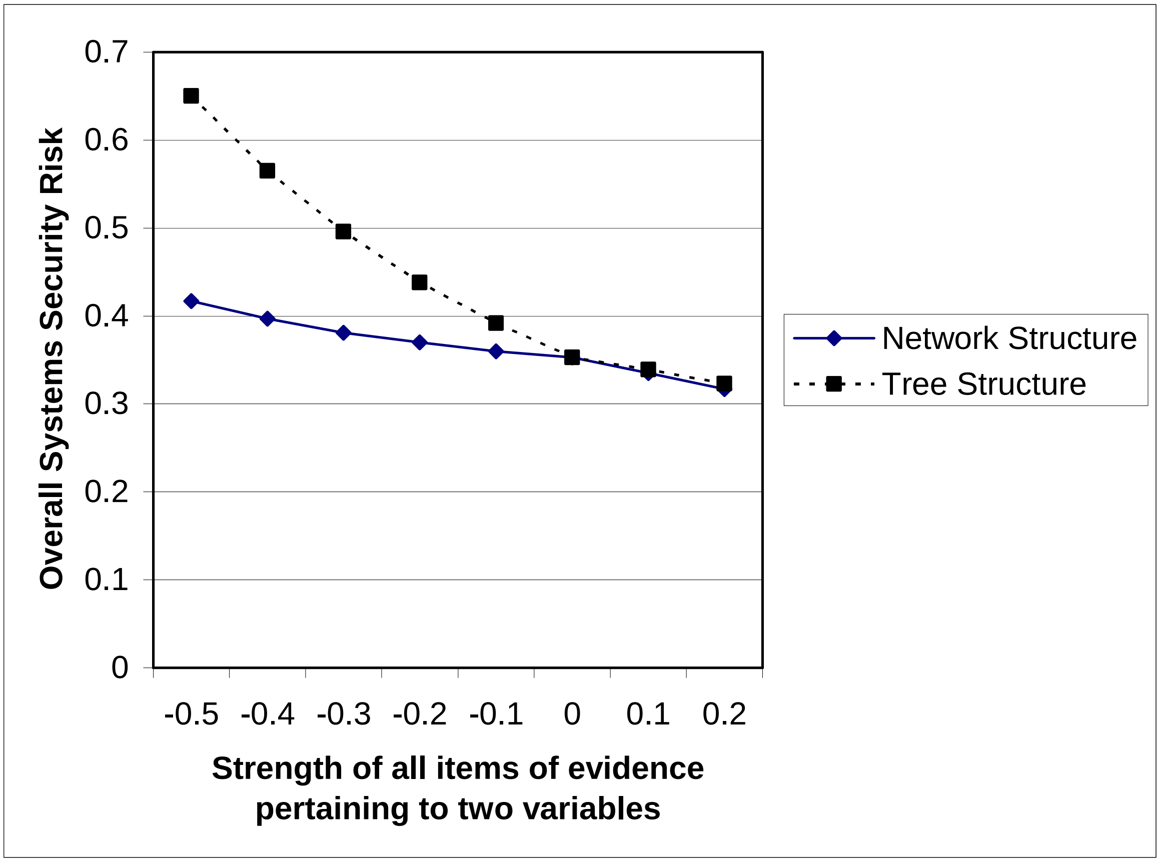


Figure 6. The impact of strength of evidence that pertains to more than one variable on the overall systems security risk that the system is not protected against unauthorized access.


Overall Systems Security Risk
Strength of all items of evidence pertaining to two variables
Network Structure
Tree Structure