

Estimating the Relative Trustworthiness of Information Sources in Security Solution Evaluation

Siv Hilde Houmb¹, Indrakshi Ray², and Indrajit Ray²

¹ Department of Computer Science
Norwegian University of Science and Technology
Sem Sælands Vei 7-9, NO-7491 Trondheim, Norway
sivhoumb@idi.ntnu.no

² Computer Science Department
Colorado State University
601 S. Howes Street, Fort Collins, CO 80523-1873, USA
{iray, indrajit}@CS.colostate.EDU

Abstract. When evaluating alternative security solutions, such as security mechanism, security protocols etc., “hard” data or information is rarely available, and one have to rely on the opinions of domain experts. Log-files from IDS, Firewalls and honeypots might also be used. However, such source are most often only used in an “penetrate and patch” strategy, meaning that system administrators, security experts or similar surveillance the network and initiate appropriate reactions to the actions observed. Such sources refers to real-time information, but might also be used in a more preventive manner by combining it with the opinions provided by the domain experts. To appropriately combine the information from such various sources the notion of trust is used. Trust represents the degree to which a particular information source can be trusted to provide accurate and correct information, and is measured as information source relative trustworthiness. In this paper we show how to assign this relative trustworthiness using two trust variables; (1) knowledge level and (2)level of expertise.

1 Introduction

Achieving the correct level of security in an application depends not only on the security level, but also on the time-to-market (TTM) and budget constraints imposed upon the system. This advocates the need for evaluating alternative security solutions. The security standard ISO 15408:1999 Common Criteria for Information Technology Security Evaluation [7] supports the evaluation of security solutions through a hierarchy of evaluation assurance levels (EAL). These levels and associated guidelines takes an evaluator through activities assessing the security level of a security solution. Risk management standards, such as the Australian/New Zealand standard for Risk Management AS/NZS 4360:2004 [1]

and its companion guideline standard HB 436:2004 Risk Management Guidelines [2], evaluate security solutions through a set of risk treatment assessment activities. However, in most cases both security standards and risk management standards relies heavily on subjective assessment by one or few assessors. Rather than having an assessor interpret information, it would be beneficial to directly make use of information from various information sources when doing security solution evaluation. Such an approach would not only simplify the process of security solution evaluation, but would also provide technique that aid evaluators by offering a way to structurally combine the large amount of information that such evaluations include.

Because the information that are available in security solution evaluations are both subjective and experience or empirical, aggregation techniques that can handle information of various degrees of uncertainty is needed. This paper describes a trust-based performance strategy for aggregating various information using information sources' relative trustworthiness. This relative trustworthiness is an expression of the ability of an information source to provide accurate information, and is assessed by examining its past and expected future performance. The expected future performance is determined by examining to what degree the knowledge and expertise level of an information source is in accordance to that required for the problem in question. Expected future performance is evaluated by looking at the currently perceived performance of an information source using the two trust variables; (1) knowledge level and (2) level of expertise.

The paper describes how to determine the information source relative trustworthiness using the two trust variables. The approach is demonstrated by an example that determines the relative trustworthiness for four domain experts and a honeypot.

The paper is organised as following. Section 2 provides a brief description of potential information sources that might be used in security solution evaluations. Section 3 describes how to determine the information source relative trustworthiness using the two trust variables. Section 4 demonstrate how to use the approach described in Section 3. Section 5 puts the work into context and Section 6 conclude the paper with some pointers to future directions.

2 Information sources for security solution effect evaluation

Information sources can be both active and passive entities, and their relative trustworthiness vary depending on the problem being assessed. When evaluating security solutions there are two main categories of information sources available; directly and indirectly observable sources. Directly observable or empirical and experience sources are sources that either have access to empirical information or that have directly observed a phenomena. Such sources have not been biased by human opinions, meaning that the source has gained knowledge and experience by observing actual events. Indirectly observable or interpreted sources includes

sources that have indirectly observed a phenomena, such as subjective expert judgments or other types of interpreted information.

Commonly used directly observable information source are real-time information sources, such as Intrusion Detection Systems (IDS), log-files from firewalls, internet gateways (routers) and honeypots [16]. Other directly observable sources are company experience repositories, public experience repositories, domain knowledge, recommendations (best practices) and related standards. Examples of public repositories are the quarterly reports from Senter for Informasjonssikkerhet (SIS) in Norway, incident and security reports and white papers from CERT, NIST, NSA and CSO, reports from the Honeynet-project [17] and other attack trend reports.

For security solution evaluation two types of indirectly observable sources are commonly used; subjective expert judgment and interpreted expert information. In subjective expert judgment the experts have directly gained knowledge and experience that they use when providing information. Interpreted expert information refers to events observed by a third party, such as another expert or a directly observable source, and given as a recommendation. In such cases, the expert interprets the information given by other sources before providing the information.

3 Determining information source relative trustworthiness

Determining information source relative trustworthiness, in the trust-based performance approach for aggregating information for security solution evaluation, is done using two trust variables: (1) knowledge level and (2) level of expertise. Before describing the trust variables and explain how they are used to determine information source relative trustworthiness, we look into what is meant by the notion of trust.

The definition of trust and distrust used in the trust-based performance aggregation approach is modified from Ray and Chakraborty (2005) [15].

Trust is the firm belief in the competence of an information source *to provide accurate and correct information* within a specific context.

Distrust is the firm belief in the incompetence of an information source *to provide accurate and correct information* within a specific context.

As can be seen by the definitions, trust is specified in relation to a particular context and might exist in some situations and not in others, as described in the ^xTrust framework by Branchaud and Flinn (2004) [4]. Trust context describes the environment, purpose, assumptions and validity of a trust relationship. The way the trust context is specified might include a variety of variables, as well as vary from case to case depending on the trust purpose, as discussed in [4]. We will not elaborate more on the trust context in this paper, but rather assume that the trust context is specified in such a way that the available information can be combined. However, the reader should note that information from different

information sources cannot directly be combined in situations where the trust context differs.

A trust relationship is usually established for some purpose between an truster A and a trustee B , and are valid in a particular time frame. A trust relationship is furthermore established under some assumptions, for a particular case in a particular environment. However, when determining the relative trustworthiness of information sources it is the information source's ability that is measured, and not an external entity's degree of trust in the information source.

3.1 Knowledge level

The trust variable *knowledge level* are used to determine the level of domain knowledge of an information source, which is measured in terms of *knowledge score*. Knowledge in this context covers facts and experience that an information source has obtain in some way, most often through either education or professional work situations. The level of knowledge is clearly a subjective measure and should therefore be assessed not only by the information source itself, but also by the evaluator or a third party that has sufficient overview of both the education and work experience for the information source, as well as being sufficiently aware of the purpose of the information that the information source is providing.

The relative knowledge score for an information source are determined by establishing a general domain relation model, specify the knowledge domain relation model for the information source and then comparing this model with the general knowledge domain model. Estimating the relative weight from the comparison might be done in a variety of ways. In the example in Section 4 we use a score-based approach that are fairly simple, but that makes it easy to observe the effects of changing any of the domain models. The knowledge score is denoted K_i , where i represent information source number i .

Figure 1 shows a general reference knowledge domain model consisting of four domains. This domain model describes which knowledge domains that are relevant when evaluating security solutions, as well as specify the internal relations or relative weight/importance between the knowledge domains. In Section 4 we give an example of a reference knowledge domain model, information source knowledge domain models and how to compare the two models to derive at the knowledge score.

As mentioned earlier, each knowledge domain have a particular importance w_{imp} and coverage c_{cov} for the security solution evaluation being performed. Both the importance and coverage weights might be assigned by any of the involved stakeholders, standards, regulations, the evaluator or similar. The knowledge domain importance is modelled as the one-dimensional array $w_{imp} = [w(1), \dots, w(j), \dots, w(m)]$, where w_j represent the importance weight for knowledge domain j , which stores these knowledge domain importance weights. The coverage is similarly modelled as the one-dimensional array $c_{cov} = [c(1), \dots, c(j), \dots, c(m)]$. The values of these arrays might be specified in the trust context or given during

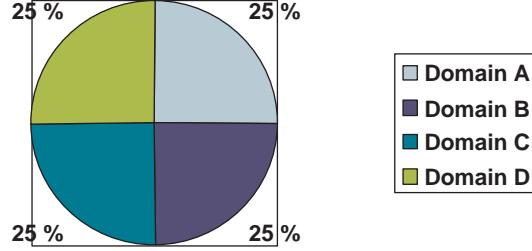


Fig. 1. General reference knowledge domain model

the evaluation process. It is often hard to assign $w(j)$ and $c(j)$ before the stakeholders or evaluator have gained sufficient overview of the involved knowledge domains.

The importance and coverage weight for knowledge domains are part of the knowledge domain relative score model, which are used to compute the knowledge score for the knowledge domain involved in the security solution evaluation. The knowledge score is determined using (3), which multiplies each knowledge domain importance weight, derived using (1), with the coverage for each knowledge domain, derived using (2). The results are then normalised over the set of knowledge domains in (5) using the knowledge domain normalisation factor $f_{knowledge}$ derived in (4).

Knowledge domain relative score model is used to derive the relative score for each knowledge domain involved in a particular security solution evaluation.

$$w_{imp} = [w(1), \dots, w(j), \dots, w(m)] \quad (1)$$

$$c_{cov} = [c(1), \dots, c(j), \dots, c(m)] \quad (2)$$

$$P_{Kscore}(K(j)) = \sum_{j=1}^m \frac{c(j) \times w(j)}{m} \quad (3)$$

$$f_{knowledge} = \frac{1}{\sum_j^m K(j)} \quad (4)$$

$$P_{relativeKscore}(K(j)) = f_{knowledge} \times K(j) \quad (5)$$

The subjective nature of assessing knowledge has some problems, such as e.g. that it requires a large amount of experience on the abilities of an information source for a third party to assess its knowledge domains accurately. We are

therefore working on establishing a set of calibration variables for the level of knowledge variable. Calibration variables in this context could e.g. be in terms of several questions targeting the same issue, but formulated in such a way that their answers would contradict if not answered accurately enough. This is a well known method used during interrogations in crime investigation.

3.2 Level of expertise

The second trust variable, *level of expertise*, are used to determine the relative level of expertise for an information source in relation to a particular security solution evaluation. As for *knowledge level*, the level of expertise is measured in terms of a score, in this case called *expertise score*. This expertise score is determined based on seed/calibration variables, which are assessed using a information source level of expertise questionnaire. Table 1 shows an example questionnaire containing an example set of seed/calibration variables. The associated categories for each of the seed/calibration variables are used to determine, in addition to the knowledge level, the relative trustworthiness for an information source. The reader should note that the categories used in this paper serves the purpose of being an example. The demonstration of its use is given in the example described in Section 4.

Variables	Categories
level of expertise	low, medium and high
age	under 20, 20-25, 25-30, 30-40, 40-50, over 50
years of relevant education	1 year, 2 years, Bsc, Msc, PhD, other
years of education others	1 year, 2 years, Bsc, Msc, PhD, other
years of experience from industry	1-3 years, 5 years, 5-10 years, 10-15 years, over 15 years
years of experience from academia	1-3 years, 5 years, 5-10 years, 10-15 years, over 15 years
role experience	database, network management, developer, designer, security management and decision maker

Table 1. Example seed/calibration variables for determining the *level of expertise*

To determine the weight that should be given to each of the seed/calibration variables, the relative importance of each of the variables for the security evaluation being performed need to be determined. The relative importance for the calibration variables are modelled as the one-dimensional array $w_{imp} = [w(1), \dots, w(k), \dots, w(l)]$, where $w(k)$ refers to calibration variable for determining level of expertise number k and l is the number of calibration variables, as described in (6). Importance in this context relates to how essential or critical

a particular calibration variable are for the ability of the information source to provide accurate and correct information. These importance weight might be provided as part of the trust context, but are also often provided during the security solution evaluation. The values might also be updated whenever new information becomes available.

During an security solution evaluation appropriate values for the calibration variables for each information source is provide. Because these variables are used to describe the information source, the values might be provided either by the information source or by a third party. Third party, in this context, does not refers to some other entity providing recommendation on a particular entity, as described in [15], but are represent knowledge and experience related to the information source. These values are then inserted into the calibration variable value array, which is modelled as the one-dimensional array $c_{exp} = [c(1), \dots, c(k), \dots, c(l)]$, where $c(k)$ refers to the provide value for calibration variable number k and l is the number of calibration variables, as described in (7).

The calibration variable score for an information source is then determined using (8), which multiplies each calibration variable importance weight from (6) with the belonging value from (7). The results are then normalised over the set of calibration variables in (10) using the knowledge domain normalisation factor $f_{experience}$ derived in (9).

Expertise level relative score model is used to derive the relative score for each seed/calibration variable from the level of expertise questionnaire used in a particular security solution evaluation.

$$w_{imp} = [w(1), \dots, w(k), \dots, w(l)] \quad (6)$$

$$c_{exp} = [c(1), \dots, c(k), \dots, c(l)] \quad (7)$$

$$P_{Escore}(E(k)) = \sum_{k=1}^l \frac{c(k) \times w(k)}{l} \quad (8)$$

$$f_{experience} = \frac{1}{\sum_k^l E(k)} \quad (9)$$

$$P_{relativeKscore}(E(k)) = f_{experience} \times E(k) \quad (10)$$

As for the level of knowledge variable, estimating an information source's level of expertise also have a high risk of bias. However, in this case one use a set of calibration variables, rather than a subjective evaluation, to estimate the level. This still does not represent an "objective" assessment because the relations between these variables is not always modelled accurately (and in this case, not at all). Aspects that might be of importance is to examine if their are any difference in relative importance between *years of experience from industry* and *years of experience from academia*. E.g. does one year from the industry have more influence on the expertise level than one year in academia, or visa versa. Another important aspect is to look into how the different age groups assess their own perceived *level of expertise*. These issues are part of an controlled experiment that we are currently performing.

3.3 Estimating information source relative trustworthiness

The result from the two trust variables; the knowledge and expertise score, is combined when estimating the information source relative trustworthiness using the estimate relative IS trustworthiness model. The initial trustworthiness is computed by the initial trustworthiness function $T(i)$, where i refers to information source number i and n is the number of information sources. This initial weight is derived by combining the relative knowledge and experience score for information source i . ε is the error function, which is used to neutralise any over and underestimation, and represent the models ability to capture experience gained on the use of the information source i . We will not elaborate more on this, but merely make the reader aware that this issue is handled in other parts of the trust-based performance aggregation approach. More information on the problem of under and overestimation or elicitation of expert judgments in general can be found in e.g. Cooke (1991) [9], Goossens et al. (2000) [11], Cooke Cooke and Slijkhuis (2003) [8] and similar sources.

After deriving the trustworthiness weight for each information source in (11), the weights need to be normalised. Normalisation is done in (12) and the relative trustworthiness normalisation factor $f_{relativeTrustw}$ is derived. The initial trustworthiness weights for each information source is then updated in (13).

Estimate relative IS trustworthiness model is used to combine the knowledge and expertise score such that the information source relative trustworthiness is derived.

$$T(i) = \sum_{j=1}^m (P_{relativeKscore}(j) \times K(j)) + \sum_{k=1}^l (P_{relativeEscore}(k) \times E(k)) - \varepsilon$$

$$f_{relativeTrustw} = \frac{1}{\sum_{i=1}^n T(i)} \quad (12)$$

$$T_{Trustw}(i) = T(i) \times f_{relativeTrustw} \quad (13)$$

$$T_{relativeTrustw}(i) = \frac{1}{\sum_{i=1}^n T_{Trustw}(i)} \quad (14)$$

Because the relative weight are normalised, trustworthiness is expressed with values in the range $[0, 1]$. The value 0 means no trustworthiness. Values close to 0 expresses little trustworthiness and values close to 1 describe high trustworthiness. Unknown trustworthiness can also be expressed, but is not covered here. However, the symbol \perp is used to express such situations.

Whenever using the relative trustworthiness weight to evaluate a security solution, the relative trustworthiness weights are first combined with the information each of the information sources has provided, and then normalised over the number of information sources.

4 Example of determining information source relative trustworthiness in security solution evaluation

We use a .Net e-commerce system to demonstrate how to derive the relative trustworthiness for information sources using the two trust variables. The information sources included in this example are the directly observable information source log-files from a honeypot and four domain experts, which are indirectly observable or interpreted information sources.

Consider the login service of the .NET e-commerce platform prototype developed by the EU-project ACTIVE [10]. To access any of the services in the platform users must login. Users login using a web browser on their local machine. The browser communicates with a web server unencrypted over the Internet using the http protocol. For more details on the login mechanism the reader is referred to Houmb et al. (2005) [12].

Typical security threats for such a login service are different types of denial of service (DoS) attacks, such as TCP SYN flooding [6] and IP spoofing attacks [5].

A potential security solution for these type of attacks is a patch to the network stack software that keeps track of the state of sessions. This is done by first sending a cookie to the client, and then removing the pending connection. If the client does not respond within a short period of time, the cookie expires and the client must re-start the request for a connection. If the client responds in time, the SYN-ACK message is sent and the connection is set up. Adding the cookie message makes it unlikely that an attacker can respond in time to continue setting up the connection. The cookie will expire on the server, and the connection attempt is closed. If the client address has been spoofed the client will not respond in any event.

Another security solution for these two DoS attacks is a filtering mechanism, which is depicted in Figure 2 and 3. The filtering mechanism has an outbound and inbound part that checks the source address, srcAddr, against a set of accepted source IP addresses stored in internalNetAddr. Rather than adding control through the additional cookie, the filtering mechanism is implemented on the server side (usually on a firewall or an internet router) and configured to block unauthorised connection attempts.

To evaluate these two security solutions the directly observable source real-time data from a honeypot and the indirectly observable information source expert opinions from 18 domain experts were used. The honeypot was set up to reflect the configuration of the .NET e-commerce platform (Windows NT 4.0 operating system and IIS 4.0). As a second layer of logging the Intrusion Detection System (IDS) Snort were used. For more information on the honeypot and its configuration the reader is referred to Østvang (2003) [14]. The group of experts used were undergraduate students at Norwegian University of Science and Technology. Further information on the collection of expert judgments is provided in Houmb et al. (2004) [13].

For the honeypot information source only the connection attempts to TCP port 80, which is intended for the web server, were considered. Logging was done

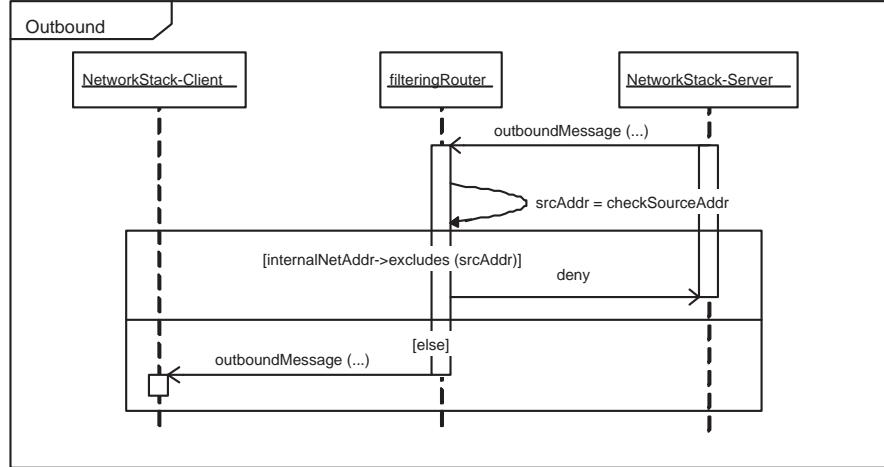


Fig. 2. Filter mechanism outbound

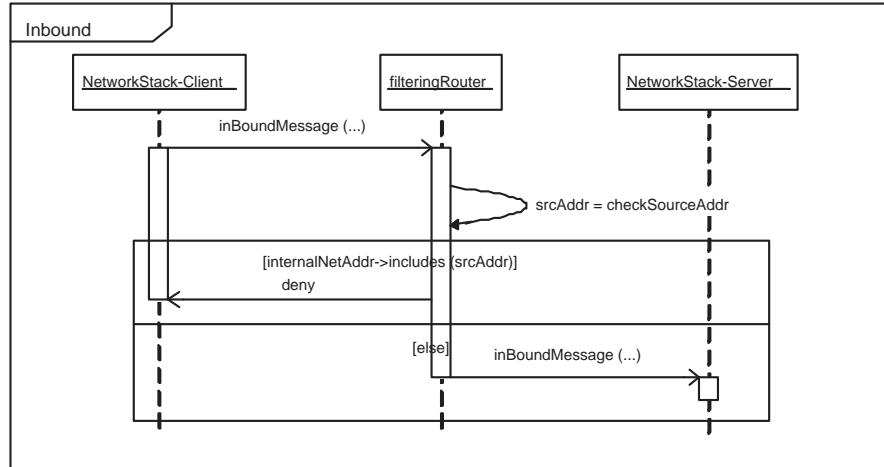


Fig. 3. Filter mechanism inbound

for the same amount of time, 24 hours, for the three different configurations: (a) system without any security solutions, (b) system with the patch to the network stack software; the cookie solution and (c) system with the filtering mechanism. The result of these three logging configurations are then used, as the information provided from the information source “honeypot”, when evaluating the two security solutions. However, in this paper we focus on how to derive the relative trustworthiness. Because “honeypot” is an observable information source

that observes fact, we assign to it the initial trustworthiness weight $T_{honeypot} = 1$ " according to (13). The value 1 indicates that the evaluator has complete trust in the ability of "honeypot" to provide accurate and correct information on number of DoS attacks. This means that the evaluator has a set of positive experience of using "honeypot". For information on how to derive such an trust weight the reader is referred to Ray and Chakraborty (2004) [15]. It should be noted that honeypots and IDSs are subject to the problem of false positives and the problem of simulating sufficiently realistic system environment and use.

Elicitation of expert judgments were done using a simple knowledge and expertise score questionnaire. The information provided on each expert for the variables in the questionnaire was then used to derive the knowledge and expertise score as described in Section 3.1 and Section 3.2. Due to space restrictions only the judgment from 4 of the 18 experts are included. For discussion on problems and possible biases related to the procedure of collecting expert judgment the reader is referred to Cooke (1991) [9] and Goossens et al. (2000) [11] and similar sources.

Expert num-ber	Calibration variable	Information provided
4	level of expertise years of relevant of education years of experience from industry role experience	medium Bsc 0 database and security management
6	level of expertise years of relevant of education years of experience from industry role experience	low Bsc 0 database
15	level of expertise years of relevant of education years of experience from industry role experience	high Bsc 0 designer, developer and security management
18	level of expertise years of relevant of education years of experience from industry role experience	low Bsc 0.5 developer

Table 2. The expertise and knowledge level questionnaire and the information provided

As described in Section 3.1 the knowledge score for an information source is determined by comparing the information source knowledge domain models with the reference knowledge domain model. The reference knowledge domain model is created by identifying the relevant knowledge domains and assessing their in-

ternal relative importance. Here the relevant knowledge domains are; security management, design, network manager, database and developer. Figure 4 shows the four knowledge domains and their internal relative importance. For demonstrational purpose the focus is put on the result of the identification, rather than discussing techniques that can be used to identify these knowledge domains.

In this example a domain expert, one of the authors, that was not part of the expert judgment panel, performed the identification based on prior experience in the domain of secure system development. Due to the subjective nature of this assessment potential biases need to be assessed. We are currently working on establishing alternative and more “objective” techniques for knowledge domain identification.

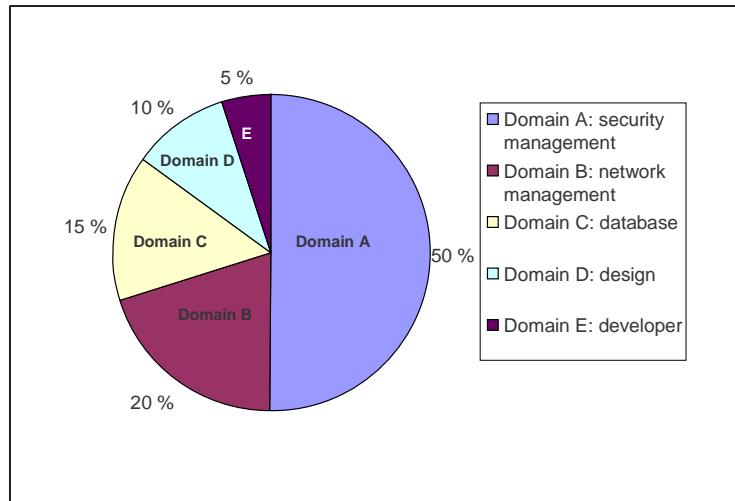


Fig. 4. The reference knowledge domain relation model for the example

The knowledge domains coverage for each expert is: 80 percentages on security management and 15 percentage on database for expert 4. 100 percentages on database for expert 6. 60 percentages for design, 30 percentages on developer and 10 percentages for security management for expert 15. 100 percentages on developer for expert 18. The knowledge level for each expert is computed using the knowledge domain relative score model from Section 3.1 and (11) from the estimate relative IS trustworthiness model

For expert 4, 6, 15 and 18 the initial knowledge score $K(4)$, $K(6)$, $K(15)$ and $K(18)$ are (the values are divided by 100 to make the computation more tractable):

$$P_{Kscore}(K(4)) = (50 \times 85) + (15 \times 15) = 4475/100 \approx 45$$

$$P_{Kscore}(K(6)) = (100 \times 1) = 1500/100 = 15$$

$$P_{Kscore}(K(15)) = (60 \times 10) + (30 \times 5) + (10 \times 50) = 1250/100 \approx 13$$

$$P_{Kscore}(K(18)) = (100 \times 5) = 500/100 = 5$$

Normalising the result is done using (4) to derive the normalisation factor $f_{knowledge}$ and (5) to update the knowledge scores. Using (4) gives $f_{knowledge} = 0.013$ and the updated approximated knowledge scores are: $K_{relativeKscore}(4) = 0.6$, $K_{relativeKscore}(6) = 0.2$, $K_{relativeKscore}(15) = 0.19$ and $K_{relativeKscore}(18) = 0.01$.

The level of expertise for each information source are derived using the calibration variables in Table 2. In this example we use three of the seed/calibration variables to determine level of expertise; *level of experience*, *years of relevant education* and *years of experience from industry*. For the calibration variable *level of experience* the importance weights using (6) are $w_{imp}(low) = 0.2$, $w_{imp}(medium) = 0.5$ and $w_{imp}(high) = 1.0$. For the calibration variable *years of relevant education* the importance weight are $w_{imp}(Bsc) = 0.2$. For the calibration variable *years of experience from industry* the importance weight is $w_{imp}(per_year) = 0.2$ for each year of industrial experience.

Using (8) the initial expertise level scores

$P_{Escore}(E(k))$ are derived: $P_{Escore}(E(4)) = 0.5$, $P_{Escore}(E(6)) = 0.2$, $P_{Escore}(E(15)) = 1.0$ and $P_{Escore}(E(18)) = 0.02$.

These initial expertise level scores are then normalised by first determining the expertise level normalisation factor using (9), which gives $f_{expertise} = 0.6$. Then the expertise level scores are updated in (10), which gives the approximate scores $P_{Escore}(E(4)) = 0.3$, $P_{Escore}(E(6)) = 0.19$, $P_{Escore}(E(15)) = 0.6$ and $P_{Escore}(E(18)) = 0.01$.

Finally, we use the estimation relative IS trustworthiness model to derive the information source relative trustworthiness. In this model one first determine the initial trustworthiness using (11), which gives the approximated values: $T(honeypot) = 1.0$, $T(4) = 0.2$, $T(6) = 0.04$, $T(15) = 0.1$ and $T(18) = 0.01$. The second step in the model is to find the relative trustworthiness normalisation factor using (12), and the third step is to derive the initial information source relative trustworthiness using (13) and normalising the result in (14). This gives $f_{relativeTrustw} = 0.7$. The resulting trustworthiness score for the information source “honeypot” is $T_{relativeTrustw}(honeypot) = 0.7$. The resulting trustworthiness score for expert 4, 6, 15 and 18 are: $T_{relativeTrustw}(expert4) = 0.1$, $T_{relativeTrustw}(expert6) = 0.1$, $T_{relativeTrustw}(expert15) = 0.1$ and $T_{relativeTrustw}(expert18) = 0.0$.

As can be seen by the result, these information source relative trustworthiness reflects the information provided on each source’s knowledge domains and level of expertise. E.g. expert 1 has two knowledge domains where one of the domains is security management, which are assigned a high level of importance. Expert 1 also has medium level of expertise. It is therefore reasonable that expert 1 are given a higher trustworthiness score than expert 18, because expert 18 have a low level of expertise and one knowledge domain for which are given a low level of importance. As also can be seen by the result, we are not able to distinguish

between expert 4, 6 and 15. This is also reasonable taking into account that their knowledge domains and level of expertise combined equals out the differences.

In security solution evaluation these information source relative trustworthiness weights are combined with the information each of the sources provide, which in this example gives the estimated security solution effect.

5 Related work

There exist a variety of trust models. However, many of these models are designed for establishing trust relationships between entities for exchange of particular information in an distributed setting, such as e.g. encryption keys or session keys. In these cases trust is measured using binary entities, such as total trust or no trust. Example of more flexible trust models is the vector trust model developed by Ray and Chakraborty [15], ^XTrust developed by Branchaud and Flin [4] and the BBK metric developed by Beth, Borcherding and Klein [3].

However, our work does not concern entities that engage in information exchange in distributed networks or other system environments. The relative trustworthiness in our model relates to information sources providing information in security solution evaluation. The information sources are mostly domain experts of some kind, and the trustworthiness is not a measure of the value of the trust relationship between a truster and some trustee, as describe in [15], but between the trustees by examine their level of knowledge and experience related to the security solutions that are being evaluated. One might use any other trust model to derive the relative measures of trust. We have, however, focused on capturing how an evaluator works when assessing security targets, such at what kind of information are being used, how are the information being used etc., and therefore our model can be used to aid such processes.

6 Conclusion

The paper describes how to derive information source relative trustworthiness for security solution evaluation. The relative trustworthiness for each information source is determined using the two trust variables (1) knowledge level and (2) level of expertise. An information source's knowledge level is measured using a knowledge score, while the level of expertise is measure using a expertise score.

It is important to note, however, that the derived relative trustworthiness of information sources still merely represent the combination of domain knowledge and human interpretation of what is important to take into consideration in a particular security solution evaluation. This means that the construction of the knowledge domain models and the assessment of the level of expertise are critical for the correctness of the results.

Further work includes implementing the approach using Bayesian Belief Networks (BBN). BBN handle large scale conditional probability computations and allows for reason under uncertainty. More information the reader is referred to Houmb et al. (2005) [12].

References

1. Australian/New Zealand Standards. AS/NZS 4360:2004 Risk Management, 2004.
2. Australian/New Zealand Standards. HB 436:2004 Risk Management Guidelines – Companion to AS/NZS 4360:2004, 2004.
3. T. Beth, M. Borcherding, and B. Klein. Valuation of trust in open networks. In *Proceedings of ESORICS 94*, November 1994.
4. M. Branchaud and S. Flinn. xTrust: A Scalable Trust Management Infrastructure. In *Proceedings of the Second Annual Conference on Privacy, Security and Trust (PST 2004)*, pages 207–218, October 14-15 2004.
5. CERT Advisory CA-1995-01. IP Spoofing Attacks and Hijacked Terminal Connections, September 1997. CERT Coordination Centre, <http://www.cert.org/advisories/CA-1995-01.html>.
6. CERT Advisory CA-1996-21. TCP SYN flooding and IP spoofing attacks, November 2000. CERT Coordination Centre, <http://www.cert.org/advisories/CA-1996-21.html>.
7. ISO 15408:1999 Common Criteria for Information Technology Security Evaluation. Version 2.1, CCIMB-99-031, CCIMB-99-032, CCIMB-99-033, August 1999.
8. R.M. Cooke and K.A. Slijkhuis. Expert Judgment in the Uncertainty Analysis of Dike Ring Failure Frequency. *Case Studies in Reliability and Maintenance*, pages 331–350, 2003.
9. Roger M. Cooke. *Experts in Uncertainty: Opinion and Subjective Probability in Science*. Oxford University Press”, 1991.
10. EU Project EP-27046-ACTIVE. EP-27046-ACTIVE, Final Prototype and User Manual, D4.2.2, Ver. 2.0, 2001-02-22., 2001.
11. L.H.J. Goossens, F.T. Harper, B.C.P. Kraan, and H. Metivier. Expert Judgement for a Probabilistic Accident Consequence Uncertainty Analysis. *Radiation Protection and Dosimetry*, 90(3):295–303, 2000.
12. S. H. Houmb, G. Georg, R. France, J. Bieman, and J. Jürjens. Cost-Benefit Trade-Off Analysis using BBN for Aspect-Oriented Risk-Driven Development. In *Proceedings of Tenth IEEE International Conference on Engineering of Complex Computer Systems (ICECCS 2005), Shanghai, China*, pages 195–204, June 2005.
13. S. H. Houmb, O. A. Johnsen, and T. Stalhane. Combining Disparate Information Sources when Quantifying Security Risks. In *1st Symposium on Risk Management and Cyber-Informatics (RMCI'04)*, July 2004.
14. M. E. Østvang. The honeynet project, Phase 1: Installing and tuning Honeyd using LIDS, 2003. Project assignment, Norwegian University of Science and Technology.
15. I. Ray and S. Chakraborty. A Vector Model of Trust for Developing Trustworthy Systems. In P. Samarati, P. Ryan, D. Gollmann, and R. Molva, editors, *Proceedings of the 9th European Symposium on Research in Computer Security (ESORICS 2005)*, pages 260–275, 13–15 September 2004.
16. L. Spitzner. *Honeypot – tracking hackers*. Addison-Wesley, 2003.
17. The Honeynet Project. The web page for The Honeynet Project. <http://www.honeynet.org/>. Accessed 27 November 2005.