A metric for trusted systems

A. Jøsang
Telenor R&D
N-7005 Trondheim, Norway, email: audun.josang@fou.telenor.no

S.J. Knapskog
The Norwegian University of Science and Technology
N-7034 Trondheim, Norway, email: svein.knapskog@item.ntnu.no

Abstract

This paper proposes a model for quantifying and reasoning about trust in IT equipment. Trust is considered to be a subjective belief, and the model consists of a belief model and set of operators for combining beliefs. Security evaluation is being discussed as a method for determining trust. Trust may also be based on other types of evidence such as for example ISO 9000 certification, and the model can be used to quantify and compare the contribution to the total trust each type of evidence provides.

Keywords

Trust, security, assurance, security evaluation, subjective logic

1 INTRODUCTION

Security evaluation is an example of a well established method for determining trust in implemented system components. The method is based on a set of evaluation criteria like e.g. TCSEC (USDoD 1985), ITSEC (EC 1992), CC (ISO 1998) or similar, and accredited evaluation laboratories which perform the evaluation under supervision of a national authority. A successful evaluation leads to the determination of an assurance level which shall reflect to which degree the TOE or system component can be trusted.

As mentioned in (Jøsang, Van Laenen, Knapskog and Vandewalle 1997), evaluation assurance does not represent the users own trust in the actual system component, but rather a recommendation from a supposedly trusted authority. In addition, the evaluation assurance is only one of several factors supporting the user's own trust in the product.

In this paper, we propose a formal model for reasoning about trust and security evaluation. Our approach is based on *subjective logic*(Jøsang 1997) which is suitable for modelling belief in general and trust in particular. It provides a metric and a set of operators for trust so that situations involving trust and trust relationships can be modelled.

2 SUBJECTIVE LOGIC

For the purpose of believing a statement about a system, we assume that it will either be true or false, and not something in between. However, it is impossible to know with certainty whether it is true or false, so that we can only have an *opinion* about it. We will express this mathematically as:

$$b + d + u = 1, \quad \{b, d, u\} \in [0, 1]^3 \tag{1}$$

where b, d and u designate belief, disbelief and uncertainty respectively. Equation (1) defines the triangle of Figure 1, and an opinion which we will designate by ω can be uniquely described as a point $\{b, d, u\}$ in the triangle.

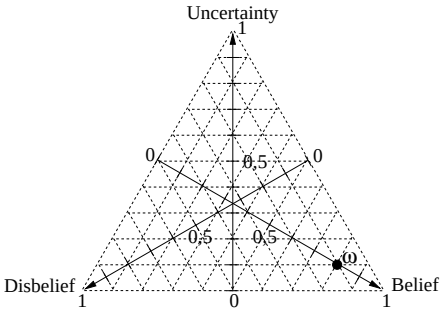

Figure 1 Opinion triangle

The operators of subjective logic take opinions about the truth of statements as variables. Opinions are subjective, and have an ownership assigned whenever relevant. Superscripts indicate ownership, and subscripts indicate the statement to which the opinion apply. For example $\omega_p^A = \{0.8, 0.1, 0.1\}$ is an opinion held by agent A about the truth of statement p, and the opinion is represented as a point in Figure 1. Due to limited space, we can not describe the operators completely, and will therefore only introduce the notation here:

Conjunction	$\omega_{p \wedge q}^A = \omega_p^A \wedge \omega_q^A$, corresponds to logical "AND"
Disjunction	$\omega_{p \vee q}^A = \omega_p^A \vee \omega_q^A$, corresponds to logical "OR"
Consensus	$\omega_{\underline{p}}^{A,B} = \omega_p^A \oplus \omega_p^B$, between independent opinions $\omega_{\overline{p}}^{A,B} = \omega_p^A \,\overline{\oplus}\, \omega_p^B$, between dependent opinions $\omega_{\widetilde{p}}^{A,B} = \omega_p^A \,\widetilde{\oplus}\, \omega_p^B$, between partly dependent opinions
Recommendation	$\omega_p^{AB} = \omega_B^A \otimes \omega_p^B$, where B recommends p to A.

3 MODELLING THE EVALUATION SCHEME

For this analysis, we will distinguish between the establishment of the trust relationships, and their subsequent role during security evaluations.

3.1 The set-up phase

An authority assigns the role of accreditor to a suitable organisation which is assumed to be trustworthy by all future participants in the scheme.

Organisations which want to be certifiers can apply to the accreditor and provide evidence to prove that they fulfil the necessary requirements. If the accreditor is satisfied it will grant a licence to the new certifier. This fact becomes evidence for everyone interested in order to trust the new certifier, as illustrated in Figure 2.a. A similar process takes place for establishing trust in evaluators, as illustrated in Figure 2.b.

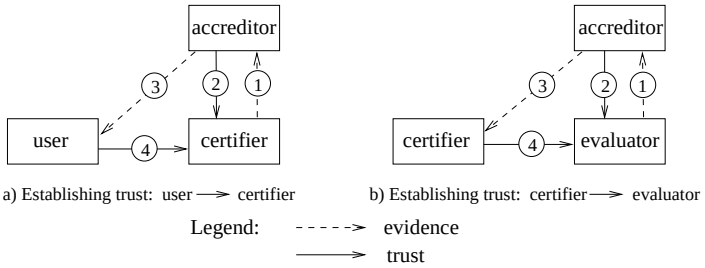

Figure 2 Set-up of security evaluation scheme

The accreditor is only checking that the applicant is fulfilling a set of requirements, and strictly speaking does not need to trust the certifier or the evaluator. However, we find that individual human members of the accrediting organisation should actually trust an applicant before granting a licence. The licensing can therefore be seen as a recommendation to the public to trust the services provided by the certifier and the evaluator.

3.2 The evaluation phase

The developer provides evidence to the evaluator who checks that the set of criteria are fulfilled. Note that the evaluator does not need to trust the actual system. It is for example possible that individual employees of the evaluation laboratory find the specified criteria insufficient to cover the security well, but nevertheless can testify that the actual criteria are met. Based on the eval-

uation report, the certifier decides whether or not a certificate of evaluation shall be issued. Note that here too, the certifier does not technically need to trust the system, but simply certifies that the evaluation has been performed correctly and that the issued certificate is consistent with the findings of the evaluation. The certificate is not a recommendation to trust the system, but only certifies that the system has been checked against a set of criteria. The user must therefore consider to which degree the certificate will make her trust the system. This chained process is illustrated in Figure 3.

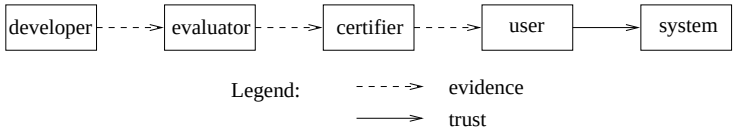

Figure 3 Evaluation and certification

4 MODELLING THE CONTEXT

The user's total trust in a system will always be based on evidence from different sources as illustrated in Figure 4.

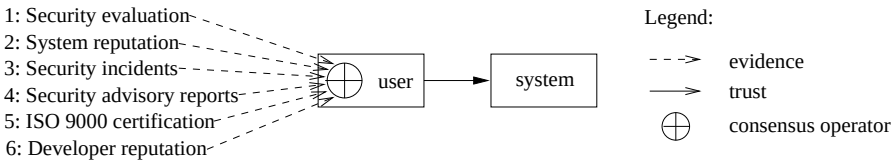

Figure 4 Contributions to trust in systems

Let A be the user who has to analyse and combine the evidence from the different sources of Figure 4. She will have to determine her opinion about the security of the system based on each type of evidence, and subsequently combine these in order to determine her general trust in the system. The consensus operator models this mental process.

In this analysis, the user will be thought of as consisting of different personalities, each faced with one type of evidence, and based on this, having a separate opinion about the systems security. Finally all the opinions can be combined together using the consensus rule to obtain what is expected to be the user's general opinion.

Our goal is to analyse and determine the user's opinion about the statement

p: "*The system will be sufficiently resistant against malicious attacks*". Let the user be A and the sub-personalities A_1 ... A_6 corresponding to each type of evidence indicated in Figure 4. A's trust in the system can be expressed as:

$$\omega_p^A = (\omega_p^{A_1} \widetilde{\oplus} \omega_p^{A_2}) \oplus \omega_p^{A_3} \oplus \omega_p^{A_4} \oplus (\omega_p^{A_5} \widetilde{\oplus} \omega_p^{A_6}). \quad (2)$$

We have assumed that $\omega_p^{A_1}$ and $\omega_p^{A_2}$ are partly dependent because system reputation can be influenced by security evaluation, and that $\omega_p^{A_5}$ and $\omega_p^{A_6}$ also are partly dependent because developer reputation can be influenced by ISO 9000 certification.

5 CONCLUSION

The presented model provides a metric and a method for reasoning about trust in the security of an IT system. For the model to be useful, it must be possible to consistently determine opinions to be used as input parameters.

We believe that the presented model can be integrated in standardisation efforts for security evaluation criteria for IT systems. This will make it possible to see the total effect of the assurance from the different types of evidence.

6 REFERENCES

EC: 1992, *Information Technology Security Evaluation Criteria (ITSEC)*, The European Commission.

ISO: 1998, *Evaluation Criteria for IT Security (Common Criteria), documents N-2052, N-2053, N-2054*, ISO/IEC JTC1/SC 27.

Jøsang, A.: 1997, *Modelling Trust in Information Security*, PhD thesis, Norwegian University of Science and Technology.

Jøsang, A., Van Laenen, F., Knapskog, S. and Vandewalle, J.: 1997, How to trust systems, *in* L. Yngström (ed.), *Proceedings of the 1997 IFIP/SEC International Information Security Conference*, IFIP.

USDoD: 1985, *Trusted Computer System Evaluation Criteria (TCSEC)*, US Department of Defence.

7 BIOGRAPHY

Audun Jøsang has a MSc in Information Security from Royal Holloway College, 1993, and a PhD from The Norwegian University of Science and Technology 1998. He is as a research scientist at Telenor R&D in Trondheim. **Svein J. Knapskog** has a MSc in telecommunication from the Norwegian Institute of Technology, 1972, and holds the position of Associate Professor at the Norwegian University of Science and Technology in Trondheim.