How to Integrate Trust Management into a Risk Analysis Process*

Peter Herrmann
Universität Dortmund, Fachbereich Informatik, D-44221 Dortmund
Peter.Herrmann@udo.edu

In order to apply suitable security services for an existing or newly designed information system, one has to perform a security analysis auditing the system for vulnerabilities, threats, and risks. Based on the audit results effective safeguards are selected, designed, and configured. The security analysis process is standardized by a set of so-called Common Criteria (CC) [8] which provides a methodology for vulnerability detection, risk assessment, and countermeasure integration. Fig. 1 delineates the main security classes and associations defined by the CC. Often, computer systems and system components store and maintain essential data and therefore are assets for their owners. These assets, however, are constantly exposed to threats by intruders, called threat agents, exploiting the vulnerabilities of the assets for attacks (e.g., a software may contain Trojan Horse code which may be utilized for eavesdropping data). Thus, the threat agents lead to security risks for the assets. The asset owners try to minimize these risks by imposing countermeasures which reduce the vulnerabilities (e.g., by a source code analysis the malicious Trojan Horse code may be detected and removed). The countermeasures, however, contain vulnerabilities themselves which, possibly, have to be reduced by other countermeasures.

A survey of security analysis approaches is provided in [1]. Typically, an audit comprises a possibly iterated series of phases concerning the following subtasks (cf. [5, 7]):

1. Identification of the system, its components, and the related principals,
2. valuation of the assets contained in the system and definition of the security objectives,
3. identification of vulnerabilities and threats,
4. valuation of the likelihood that threat agents exploit the vulnerabilities performing a successful attack.
5. assessment of the resulting risks,
6. planning, design, and evaluation of suitable countermeasures,
7. iteration of the audit of the system extended by the selected countermeasures starting from step 3.

In this audit, the values of the assets are usually not described by concrete values in Euros or US$ since it is often very difficult to estimate the exact damage from an attack. Instead, standards (e.g., [3, 8]) define more abstract security levels rating the potential damage (e.g., the security level 'maximum' should be assigned to an asset if its breakdown leads to total collapse of the institution owning the asset). Similarly, the likelihoods of successful attacks, which mainly depend on the used countermeasures, are also described by distinct levels. From the security levels of the assets and the likelihood levels of successful attacks, one computes the levels of the corresponding risks (cf. [4]). If the owner can tolerate all existing risks, one can stop the security analysis process at this point. Otherwise, one has to integrate countermeasures. Since the countermeasures are also vulnerable against attacks, the audit of the extended system is iterated which may lead to countermeasures protecting countermeasures.

The Common Criteria also define a concept of trust in which the owner of an asset has to trust that the selected countermeasures reduce the risks of the protected asset as desired. This trust can be built up by applying system evaluations (i.e., the audits mentioned above) which again have to be trusted by the asset owner.

*In Proceedings of the 2nd Internal iTrust Workshop on Trust Management in Dynamic Open Systems, London, 2003.

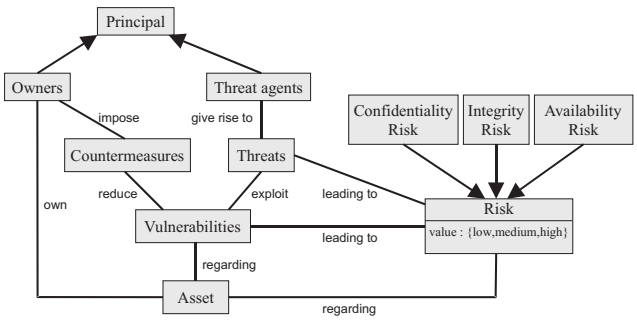

Figure 1. CC security classes

In our opinion, this trust concept, however, is not sufficient. It is basically centered on the trust in a security analysis method but not on the trust in parts of the audited system. System entities which may be trusted by an asset owner comprise the following parties:

- The group of principals with access to the asset who all may be considered as benevolent,
- an asset itself which may be free of vulnerabilities to be exploited for certain attacks,
- a countermeasure which may protect an asset sufficiently and is immune against attacks on itself relaxing the protection.

By taking trust relations between the asset owner and these parties into account, one can reduce the effort of a security analysis significantly. If one believes that all people with access to an asset are not intending certain attacks, that the asset is immune against these attacks, or that it contains sufficient countermeasures, one can omit further analysis of the corresponding risks.

In order to integrate the trust of the asset owner into the auditing process, we assume that the trust relationships are expressed by so-called trust values. In [9], Audun Jøsang defines trust values each consisting of three probability values. Two values state the degree of belief or disbelief in an entity while the third one describes uncertainty. Trust values can be computed from the number of positive resp. negative experiences with the entity to be trusted by special metrics (cf. [2, 11]). Moreover, one can include recommendations by third parties into the computation of trust values (cf. [10, 6]).

We detected two principal ways to integrate trust values into the auditing process. In the first approach, the auditing process is extended by considering trust values in the risk level computation. In particular, one alters the calculation of the likelihood that successful attacks are carried out. Currently, this likelihood depends on the structure of the asset and on the amount of protection granted by the countermeasures. Here, we can also consider the trust values as another factor. As higher the trust in the good-naturedness of the involved parties is, as lower the likelihood will be assumed. In consequence, the risk level will also decrease if the trust in the involved parties is high. Of course, in this approach we make our decisions conditional upon perceived risks instead of real risks as intended by the Common Criteria.

In the other approach, we keep the auditing process unchanged but make the decision which risk can be run and which not, dependent on the trust in the parties. In particular, we can define mappings relating the trust values with risk levels to be tolerated by the asset owner. According to these mappings, an asset owner should be willing to take as greater risks as higher the belief in benevolent behavior of the involved parties is.

All in all, we prefer the first approach. As a disadvantage, it extends the auditing process and uses perceived risks. This, however, is outweighed by the advantage that, in contrast to the second method, the decision, which risks can be taken, is not influenced by the audit. The willingness to run certain risks should only depend on the preferences and personalities of the asset owners but not on certain statistically computed parameters (i.e., the trust values).

References

[1] R. Baskerville. Information Systems Design Methods: Implications for Information Systems Development. *ACM Computing Surveys*, 25(4):375–414, Dec. 1993.

[2] T. Beth, M. Borcherding, and B. Klein. Valuation of Trust in Open Networks. In *Proceedings of the European Symposium on Research in Security (ESORICS)*, Lecture Notes in Computer Science 875, pages 3–18, Brighton, 1994. Springer-Verlag.

[3] Bundesamt für Sicherheit in der Informationstechnik, www.bsi.de. *IT Baseline Protection Manual*, 1999.

[4] R. Courtney. Security Risk Assessment in Electronic Data Processing. In *AFIPS Conference Proceedings of the National Computer Conference 46*, pages 97–104, Arlington, 1977. AFIPS.

[5] P. Herrmann. Information Flow Analysis of Component-Structured Applications. In *Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC'2001)*, pages 45–54, New Orleans, Dec. 2001. ACM SIGSAC, IEEE Computer Society Press.

[6] P. Herrmann. Trust-Based Protection of Software Component Users and Designers. In P. Nixon and S. Terzis, editors, *Proceedings of the 1st International Conference on Trust Management*, LNCS 2692, pages 75–90, Heraklion, May 2003. Springer-Verlag.

[7] P. Herrmann and H. Krumm. Object-oriented security analysis and modeling. In *Proceedings of the 9th International Conference on Telecommunication Systems — Modelling and Analysis*, pages 21–32, Dallas, Mar. 2001. ATSMA, IFIP.

[8] ISO/IEC. *Common Criteria for Information Technology Security Evaluation*, 1998. International Standard ISO/IEC 15408.

[9] A. Jøsang. An Algebra for Assessing Trust in Certification Chains. In J. Kochmar, editor, *Proceedings of the Network and Distributed Systems Security Symposium (NDSS'99)*. The Internet Society, 1999.

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

[11] A. Jøsang and S. J. Knapskog. A metric for trusted systems. In *Proceedings of the 21st National Security Conference*. NSA, 1998.