Towards solving the data problem in measurement of organizations' security

Steffen Weiß, Klaus Meyer-Wegener

University of Erlangen-Nuremberg,
Department of Computer Science, Datamanagement Systems
Martensstraße 3
91058 Erlangen
Steffen.Weiss@informatik.uni-erlangen.de
Klaus.Meyer-Wegener@Informatik.uni-erlangen.de

Abstract: Awareness of security has risen during the last years. As a result, the question of adequate protection against security risks increased, too. Management wants to decide whether and how to invest in this protection. As a result, quantitative statements about information-security risks are needed. Existing approaches in this domain either rely on guessed data or do not answer the question in a quantitative way. We think that this is due to the fact that no approach separates information that can be provided by a central organization (e.g. known attacks, available controls, and a control's probability of protection) from information which must be provided individually (e.g. the controls installed). We have developed an approach that employs this separation and allows quantitative assessment of security with the help of a model. This model is presented here with a special look at the separation.

1 Introduction

There is no longer any doubt that information security is an important aspect for organizations. On the one hand this is probably due to studies (e.g. [AH04], [SY05]) showing the potential of aggression. On the other hand, security holes are no longer a "dark science," but are reported e.g. in newspapers [FA06]. As a consequence, awareness in organizations has risen.

One of the first questions asked by management is usually: "Are we adequately protected?" This is due to the fact that under-protection can lead to large damages. However, over-protection is not good either from an economic point of view: Even if damages can be dramatically limited with the help of controls, expenses due to the costs of controls must not be neglected. Thus an adequate proportion of protection is needed—and approaches helping to identify this proportion or even better, adequate controls. This requires that reliable statements about security are possible, based on traceable, quantitative statements. However, existing approaches are not quantitative or do not provide traceable results.

In this article, we present an approach solving this problem. It separates information that can be provided by a central organization (e.g. known attacks, available controls, and a control's probability of protection) from information which must be provided individually (e.g. the controls installed). This separation allows quantitative assessment of security with the help of a model. This model is presented here with a special look at the separation.

The article is structured as follows: In chapter 2, an overview of related work is given and the main problem is addressed. Chapter 3 provides a solution for this problem. This solution is described in more detail in a presentation of (parts of) our data model (chapter 4). Finally, the benefits of this approach and some future research work are discussed in chapter 5.

2 Related work

Attack trees ([NST04], [Sc00]) model all possible attacks against a system which can be performed by an attacker, with the root node being the final goal. Conclusively one node in the tree is one possible attack. Although first ideas are given on how an assessment can be done (compare e.g. [Sc00]), a quantitative assessment is not the purpose of these trees. Moreover, there is no easy or intuitive way to model controls and their influences. Still, the tree gives an idea what modeling may look like.

[Li93] discusses taking over models from the reliability theory to security. Some important questions are identified which need to be answered before the approach can be taken further. Moreover, some types of attacks are discussed in some more detail. However, the authors themselves admit that they are far from having a modeling theory that allows allocating quantitative measures to operational security.

The IT Baseline Protection Manual (BPM) [BS05a] contains standard security safeguards, implementation advice, and aids for numerous IT configurations which are typically found in IT systems today. Besides, it contains threats, modules (typical areas in which IT assets are employed), and a procedure to "assess" security and audit the result. However, the BPM is not directed to quantitative modelling of security but rather to technical modelling. In addition, the "auditor's judgement" finally determines whether controls are regarded adequate. Thus a traceable, quantitative assessment of security is not possible.

Similar problems occur with ISO/IEC 27002 (previously published as ISO/IEC 17799 [IS05a]; similar to BS 7799-1). There is also an aligning assessment standard—ISO/IEC 27001 [IS05b] which has been developed out of and is very similar to BS 7799-2. This standard defines fitness of the Information Security Management System (ISMS), that is, the security process of the organization is checked. However, assessment is performed indirectly and not quantitatively. More recent standards (e.g. BSI-Standard 100-1 [BS05b]) have the same problem. None of these approaches allows a traceable and quantitative assessment of security.

[Ja07] suggests measuring security by measuring security indicators. Examples mentioned are "spam not detected/missed," "viruses detected in user files on servers or desktops" etc. The NIST SP 800-55 [SBS03] gives more abstract examples. Even if indicators are quantitative, some problems arise with these approaches. First, some indicator cannot be measured easily—a good example is "spam not detected/missed." Second, the meaning of an indicator in the context of the organization is not clear. Thus, saying something about security of a whole organization based on these indicators is quite difficult. Consequently, a traceable quantitative statement about an organization's security is not possible.

An important concept for quantitative assessment in commercial information technology is ALE (annual loss expectance; see [NBS79]). ALE is calculated as

ALE = Impact (Dollars) x Frequency (of occurrence per year)

This model gives a first, intuitive understanding of security evaluation. It is based on data that characterize the security risks of an organization. Yet Soo Hoo [So00] says that there is a "data crisis," meaning that there are not enough or no adequate data for the input parameters. Consequently, data can only be obtained as a guess.

Another important concept in (quantitatively) measuring security is (Information Security) Risk Assessment. Examples are NIST 800-30 [SGF02] and Mehari [CL04]. Mehari contains some intermediate steps in calculation and a sophisticated description how to carry out measurement in an organization. Yet the basic concept does not bear a significant difference (explained on basis of NIST 800-30): Threat likelihood and threat impact are inputs for the assessment of risk. Both are assessed on a scale with 3 units: 1.0 for high, 0.5 for medium, and 0.1 for low likelihood, as well as 100 for high, 50 for medium, and 10 for low impact. The product of these two factors along with the predefined thresholds for the product determines the resulting risk level. Other approaches for example use 5 units each. Even quantitative risk assessment approaches (compare e.g. the IBM approach in [Ba93]) align with this principle. [NFK05] presents the idea for a process-based risk assessment. Details about how to proceed are missing, however. All in all, the risk assessment approach allows a good overview of security if adequate scenarios for the system under investigation are assessed. Yet it does not suffice, because input and output are not detailed enough. Moreover, the reasons why a specific scale value is taken are very fuzzy. Thus, results are not traceable.

The presentation of related work has shown that there are only a very limited number of approaches dealing with quantitative measurement. Moreover, all approaches that are somehow directed to quantitative modelling (ALE and risk assessment) *lack availability of statistical data*. Also other authors have already realized this problem (e.g. [NFK05] and [So00] calling it "data problem"). Since these data are necessary as a basis for traceable assessment, a traceable quantitative statement about an organization's security is nearly impossible.

Most risk assessment and ALE-based approaches rely on data given by experts (compare e.g. [We05]). These experts can for example use surveys (e.g. [AH04]) as basis for assessment. This somehow seems to solve the data problem, as data may not be directly

available and the experts' guesses can theoretically regard all circumstances. However, traceability of resulting values is bad.

Soo Hoo presented some reasons for the data problem [So00]: For example, he speaks about a missing consensus on the specific indicators to be monitored and a lack of a consistent terminology. Already this example implies that core of the data problem is a lack of concepts e.g. which data to provide. Missing data is only an after-effect of this lack.

3 How to solve the data problem

3.1. Concept

The main reason why none of these approaches finally succeeds is that two completely different aspects are regarded as one thing: "Information" on the general risk situation and "information" on how a particular organization protects itself against these risks.

A real-world example is used to illustrate the difference: An organization reported 4 virus incidents last year, but only 2 in the year before. Even if the numbers can be trusted, it does not say anything: First, it can be due to an increase in number or a higher sophistication of attacks against the organization. Second, it can be due to sloppy installation of virus-scanner updates in the organization.

We explicitly exclude "abnormal situations" which impose high numbers and high sophistication of attacks on an organization. Examples for such situations are publishing companies shortly before the release of famous new books or videos. These situations are even more difficult to model than "usual situations." While even the measurement of security of organizations in usual situations is not yet solved, regarding more difficult situations does not make sense.

Under this assumption, there are two basic reasons for a higher number of virus incidents: First, the general attack situation has changed (e.g. more attacks). Second, the protection of the organization has become worse. Besides, also combinations are possible—e.g. more attacks and declined control quality.

In current statistics, separation of these aspects is missing or at least very rudimentary. As a result, nobody can give a statistically founded value for the number of attacks. Thus, a very important aspect in solving the data problem is distinction between information describing the general security situation and information describing the individual security situation. Provided by a central organization, general information holds publicly accepted knowledge and gives a common basis for assessment. The central organization—for example the German Bundesamt für Sicherheit in der Informationstechnik (BSI) or a Cert (Computer Emergency Response Teams)—has more resources and more knowledge than e.g. a small organization. Thus it can provide the necessary information with limited effort.

Also statistical values (being part of the general information provided) can be published more easily. One main reason for this is that the number of attacks an organization is faced with is not confidential—or at least by far not as confidential as the number of successful attacks. Thus it is more likely that organizations publish these values.

Note that we concentrate on past or current data in this article. As far as we see, forecasting is possible. However, details of forecasting exceed this article by far and it is important to settle the basic model before discussion of additional functionality is started.

The *individual information* is necessary to model the individual effects for organizations in an attack situation. The most important aspect is probably the existence (or non-existence) of controls.

The separation requires exact definition of what is provided centrally and what is provided individually. Moreover, an algorithm must be described that combines the information to meaningful results. A model is needed for this.

3.2. Precision of separation between general and individual information

Statistical values have been the main aspect of interest so far. However, there is more: "Structural information" is information about entities in the security model and the relations among these entities. Examples are controls and attacks, as well as the relation between attacks and controls which states that a controls protects against an attack. This information is at least as important as statistical values. Structural information should be provided centrally, too, out of two reasons: First of all much domain knowledge is needed to write down this information. Thus it is nearly impossible (and also inefficient) that it is written down by each organization individually. Second, a common basis for assessment is given and thus comparability of results is better.

Summarizing the solution and defining it exactly, there is a distinction between two types of information:

- Centrally provided information which can be further subdivided into structural information and (centrally provided) values. Structural information describes the entities of a security model (e.g. attacks, controls) as well as relation between these entities. An example is a control "virus scanner" protecting against an attack "virus is executed". (Centrally provided) values are figures about the general situation of attack and defending. Examples are the number of virus attacks or the probability that a control (if installed properly) protects against an attack. Organization-specific aspects—e.g. whether a control is installed nor not—are not included in centrally provided information.
- Individually provided information consists of figures about the individual situation of attack and defending. An example is whether an organization has established a specific control or not.

4 Overview of the data model

4.1. Basic model

Based on the general idea of separation between centrally and individually provided information, we start with a basic yet intuitive security model: There are possible attacks against the organization. If one of these attacks is carried out, there are usually controls which protect the organization and repel the attack.

However, controls are not perfect, so some attacks harm the organization's assets and cause damage. Figure 1 presents a graphical presentation of this intuitive understanding of security.

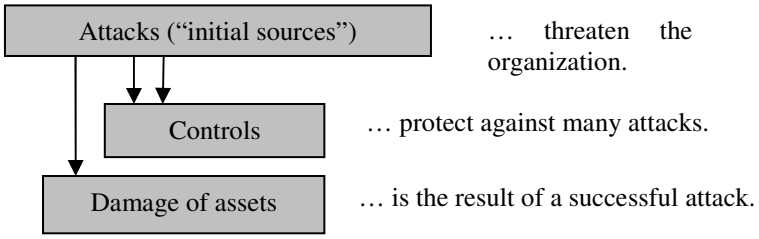

Figure 1: The basic form of a security model

4.2. Definition of terms

The interpretation of the terms in the basic model may vary. Thus, the three main terms (attack, control, and damage) must be defined before going into the details of the model. In addition, the term scenario will be defined as it is later needed in the model.

1. **Attack**: An attack is a deliberate act with the potential to harm a system or an organization. Attacks are carried out in **steps**—e.g. "virulent e-mail received by victim" and "virulent mail executed by victim." In contrast to attacks, incidents are non deliberate acts to harm a system or an organization. As far as we can see, all concepts mentioned here align also for incidents, however we mainly focus on attacks.
2. **Control:** According to [IS05a], controls are means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature.
3. **Damage**: A damage is a reduction of an asset's value for the organization that owns it. Damages are assessed in the three different dimensions of security (*availability*, *confidentiality*, and *integrity*) and affect assets.
   According to [IS05a], an **asset** is anything that has value to an organization. Assets include physical objects like computers or mobile phones, but also non-physical objects like data. This can be for example customer data, patents, or part lists.
4. **Scenarios**: Many different definitions of a scenario exist. In our opinion, a scenario

is a successful step of attack which leads to a damage—e.g. “virulent mail executed by victim”.

Due to the statistical understanding of security it is necessary to mention that terms are understood here from an ex-ante point of view. So, attacks are *possible* deliberate acts to harm a system or organization and steps of attacks are *possible* situations that can occur. The same is true for controls (which *can* protect), damages (which *can* appear), and scenarios (that *can* occur).

Regarding statistical values which are needed for this model, one additional note is necessary: The ex-ante point of view does not necessarily have impact on the values used. They may be values of past periods, the current period, or of future periods. In case of values of future periods, values will be extrapolations based on past data of values.

4.3 Basic structure of the UML model

Based on the basic model presented in section 4.1 and the definition of terms in section 4.2, we have developed a UML class model. The entities in this model are *Scenario*, *Control*, *Damage*, and *StepOfAttack*. Attacks are composed of steps of attack and are not modelled separately.

These entities are connected with relationships:

- As defined above, a *Scenario* is a successful *StepOfAttack*. Thus, S*tepOfAttack* is a generalization of *Scenario*.
- There is a n:m relationship between *Scenario* and *Damage* because a *Damage* can be due to different *Scenario*s and a *Scenario* can have more than one possible *Damage*.
- The definition of attack already included the need to model steps of attacks. One step after the other must be executed so that an attack finally succeeds. Execution can be either triggered by the attacker (e.g. sending a virus) or by the victim (e.g. opening a mail). This step-wise procedure can be modelled by a succession on the S*tepOfAttack* entity. We call the attribute entity of this relationship *AttackSuccession*. To be exact, *Controls* protect against realization of these steps of attack. Thus, there is a relationship between the *AttackSuccession* attribute entity and the *Control* entity. As it is described later, this relationship (called *Protection*) has attributes, too. For example it has a probability that the control works. Modelling influence of more than one control against an *AttackSuccession*s is not easy to model because it must be described how controls are combined. Due to space limitation we cannot explain the according model here and assume for simplification that exactly one control is assigned to an *AttackSuccession*.
- There is also a relationship between *Damage*s and *Control*s, indicating that controls protect against damages. This relationship is quite complex, too: Due to the installation of controls, *Damage*s can be decomposed into more detailed *Damage*s. For example, it is possible to model the two damages “data from hard

disk lost, but restored from backup" and "data from hard disk finally lost since there is no (usable) backup" instead of "data of hard disk lost (with status of backup not known)." However, the more detailed structure of *Damage* and the relationship will not be explained here. (In the UML model of Figure 2 we use an association without cardinality restrictions to model the fact that details of the relation are omitted here.)

The complete model (also containing details described in section 4.4.) will be presented in Figure 2.

4.4 The UML model in more depth

To get a better understanding of separation between centrally provided information and individually provided values with the help of our model, some more details of our model are given.

First of all, it is known from reality that controls protect against realization of steps of attack with a given probability. For example, it is known from investigations (e.g. [CA07]) that the best virus scanners have a detection rate of approx. 99.45% of all viruses under optimum working conditions. Similar investigations provide similar values. Without regarding details of these values, this sentence already contains much information:

- It implicitly assumes existence of two steps of attack—one (less sophisticated) step of attack before the virus scanner takes action ("virulent e-mail is received on desktop computer") and one that is taken after passing the scanner ("virulent e-mail is stored on desktop computer").
- It states that the first step of attack can be continued by the second one. Thus, there is an *AttackSuccession* "passing virus scanner" between the first step of attack and the second one.
- It states that a *Control* "virus scanner" exists, protecting against this succession between steps of attack.
- It states that there is a *Protection* relationship between "virus scanner" and the *AttackSuccession* "passing virus scanner" which is attributed with the probability of protection (99.45%).

Bullets 1 to 3 contain structural information. They are provided centrally as they are identical for every organization. Bullet 4 also contains structural information, but it further contains a (centrally provided) statistical value: the (maximum) probability of protection (99.45%).

In addition to centrally provided information, individually provided values must be included in the model. The need to take into account the status of installed controls is the main reason for this. During development of the model we followed the rule that it should be possible to individually adopt each centrally provided statistical value. In this case only the (maximum) probability of protection is targeted by this rule. Thus, there is room in the model to provide an individual adoption factor and a reason for the adoption

of the centrally provided value. In case of the (maximum) probability of protection, this adoption factor allows to model the fact that the control is not established to 100%. For example in case there is no virus scanner, an adoption factor of 0 must be assigned. In case only low-grade virus scanners are installed, an adoption factor could also be necessary (compare e.g. the "overall detection rate" of virus scanners tested in [CA07]).

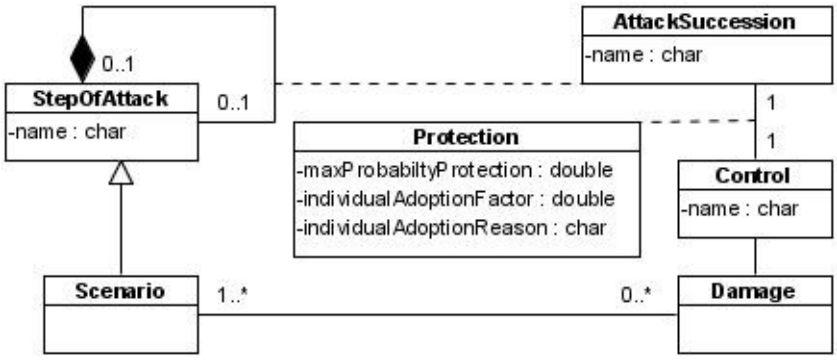

Figure 2: A more detailed overview of the UML model

In the explanation of this example, some attributes of the entities presented in section 4.3 have implicitly been named. For the completion of the UML model, we include these attributes in an extended version of the model (see Figure 2). A UML instance model, describing the example given above is presented in Figure 3.

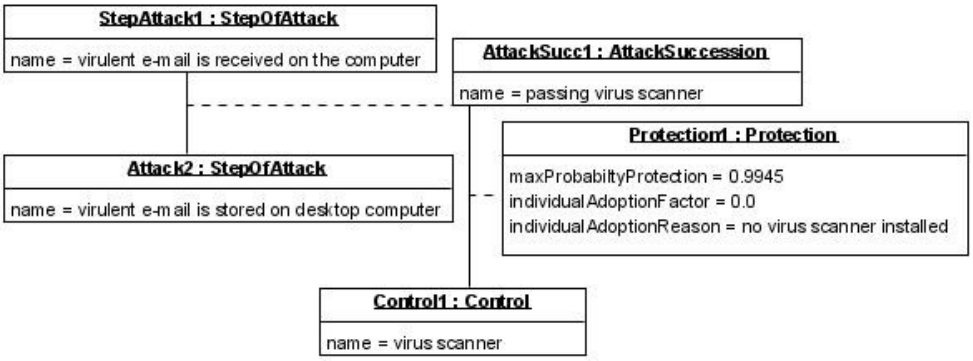

Figure 3: UML object model of the example explained in section 4.4

4.5 Calculation and completion of the example

In section 4.4, the model for protection against a step of attack was discussed. Sticking to this example, a centrally provided value of 99.45% was given. This centrally provided value must be multiplied with the individual adoption factor to get the resulting

probability of protection. In case there is no virus scanner installed, the adoption factor is 0 and thus protection probability is 0 • 0.9945 = 0. If for example only half of the computers are protected by (good) anti-virus software, an individual adoption factor of 0.5 is adequate if the rate of attack can be assumed to be equal for the computers under investigation. In this case, the resulting probability of protection is 0.5 • 0.9945 ~ 0.497. If for example Microsoft Live Oncare is used (a low-grade virus scanners according to the investigation [CA07]), an individual adoption of approx. 83% can be extracted from the statistics. Also combinations are possible—e.g. low-grade virus scanners *and* only half of the computers protected by anti-virus software. In this case, the two individual adoption factors (0.5 and 0.83) have to be multiplied. The resulting factor (0.415) is used as individual adoption factor.

The exact separation between different influences on security becomes already visible in this small snippet of reality: The magnitudes of the resulting values are given by the centrally provided values. The individual adoption can then be used for a fine tuning of the values—regarding the individual influences. However, the benefit of the model is not limited to a traceable assessment of single steps of attacks or transitions between the steps. Also the effect of succeeding steps of attacks can be modelled: An additional step of attack "virulent e-mail opened" is added to the example to demonstrate this function. The resulting probability of protection for the AttackSuccession between "virulent e-mail stored on desktop computer" and "virulent e-mail opened" is supposed to be 0.3. Assuming that only half of the computers is protected by (very good) anti-virus software (as calculated above, the resulting probability of protection equals 0.497) protection against this succession of steps of attacks is 1 – (1–0.497) • (1–0.3) ~ 0.648. Assuming further that there are no additional steps of attack, this value is protection against a whole attack.

The UML model of Figure 2 is limited to modelling protection against steps of attacks. In the complete form of the model however, there is an additional possibility: the "initial step" of attack is modelled, being the step of attack which has no predecessor. Sticking to the example given above (where we limited to model 3 steps of attacks), this is the step "virulent e-mail received on desktop computer." For this step of attack, a rate of occurrence can be given. Statistics to support these values already exist—compare e.g. the monthly security report of DATEV eG [DA07]. The resulting rate of an attack including all controls is simply a product of the rate for the initial step of attack and the complement of the probability of protection. So, in case of rate $\lambda = 10/a$ (10 per year—a fictitious value) and probability of protection $p = 0.648$ (see above), the resulting rate of the attack being successful is $10/a \bullet (1–0.648) = 3.52/a$.

In the example given above, this rate is valid for the step of attack "virulent e-mail opened." If a virulent mail is opened, it can cause damage. Thus, it makes sense to define this step of attack as a scenario. In this case, the resulting rate of attack can be taken over to the scenario—showing that a traceable, quantitative assessment of scenario occurrence is possible with our approach.

Note that centrally provided values as well as individual adoption factors provided here are only first suggestions. However, this is enough to show the idea. Moreover, in-depth investigations would demand a huge amount of space which is not available here.

Rate of scenario occurrence is one of the values which are interesting for management. ALE-based assessment and risk assessment use this value. Without the model suggested in this article, none of these approaches could tell in depth how this value is to be assessed. Thus, the approach presented here extends the existing approaches, even though one might argue that structural information is not yet provided or that not all values needed are available.

5 Future work

In this article, we have discussed existing approaches to measure the security of organizations. The main problem of these approaches was the complete lack of statistical assessment of security or at least the problem to get adequate data for assessment. These deficits were traced back to the fact that there is no separation between centrally provided information and individual adoption.

Separation of these types of information and values requires a model combining them to meaningful results. We have presented the core of the security model we have developed to perform this combination. With the help of a small example, we have shown that traceability of security measurement is much better than with existing approaches. We have also shown that values needed as input for the model are already available in many cases. Even if one argues that values are not yet available in some cases or that central information is not yet provided, it is evident that traceability of security assessment increases with the approach presented.

Nevertheless, there is some more work needed to complete the model. While we have already completed the data model and have already performed some assessment of real-world examples, further investigation of real-world examples is necessary to show that this model reflects the reality. Moreover, we have to describe the process of how to build the model in more depth. For example, we want to describe how one can extract centrally provided structural information from existing documents. Moreover, we also want to make some suggestions for predictions and give in-depth ideas for assessment of individual adoption factors.

Literature

[AH04] Australian High Tech Crime Centre: Australian Computer Crime and Security Survey, 2004.

[Ba93] Bhaskar, K. N.: Computer security threats and countermeasures, NCC Blackwell, Manchester a.o., 1993.

[BS05a] Bundesamt für Sicherheit in der Informationstechnik: IT Grundschutzhandbuch. Bonn, 2005.

[BS05b] Bundesamt für Sicherheit in der Informationstechnik (publisher): BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) Version 1.0, 2005.

[BS05c] Bundesamt für Sicherheit in der Informationstechnik (publisher): BSI-Standard 100-2 IT-Grundschutz-Vorgehensweise Version 1.0, Bonn, 2005.

[BS05d] Bundesamt für Sicherheit in der Informationstechnik (publisher): BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.0, Bonn, 2005.

[CA07] Clementi, A., Augusten, S.: Die besten Virenwächter. In: Schmitz, P. (chief editor): Information Security, issue 3/07, 2007; p. 32–37.

[CL04] Club de la securite des systemes d´information francais (Clusif) (publisher): Mehari V3 Concepts and Mechanisms, 2004.

[DA07] DATEV eG: Sicherheitsreport, 2007. http://www.datev.de/portal/ShowPage.do?pid=dpi&nid=2522&zg=n

[FA06] Frankfurter Allgemeine Zeitung: Erste Sicherheitslücke in Windows Vista entdeckt. Issue of 28th December 2006.

[IS05a] ISO/IEC: Information technology – Security techniques – Code of practice for information security management (ISO/IEC 17799, final draft), 2005.

[IS05b] ISO/IEC: Information security management system – Requirements (ISO/IEC 27001: 2005).

[Ja07] Jaquith, A.: Security Metrics Replacing Fear, Uncertainty, and Doubt. Addison-Wesley, 2007.

[Li93] Littelwood, B. et.al: Towards Operational Measures of Computer Security Towards Operational Measures, J. Computer Security, vol. 2, nos. 2/3, p. 211–229, 1993.

[NBS79] National Bureau of Standards: Guidelines for Automatic Data Processing Risk Analysis (FIPS PUB 65). 1979.

[NFK05] Nowey, T., Federrath, H., Klein, C., Ploessl, K.: Ansaetze zur Evaluierung von Sicherheitsinvestitionen. In: Sicherheit 2005. Beiträge der 2. Jahrestagung des GI-Fachbereichs Sicherheit, Lecture Notes in Informatics (P-62). Federrath, Hannes. Bonn: Köllen-Verlag; 2005; p. 15-26.

[NST04] Nicol, D. M., Sanders, W. H., Trivedi, K. S.: Model-Based Evaluation: From Dependability to Security. In: IEEE transactions on dependable and secure computing, vol. 1, no. 1, January-March 2004; p. 48–65.

[Sc00] Schneier, B.: Secrets and Lies – Digital Security in a Networked World. John Wiley & Sons, New York a.o., 2000.

[SGF02] Stoneburner, G., Goguen, A., and Feringa, A.: Risk Management Guide for Information Technology Systems (NIST SP 800-30). Washington, 2002.

[SBS03] Swanson, M., Bartol, N., Sabato, J., Hash, J., Graffo, L.: Security Metrics Guide for Information Technology Systems (NIST SP 800-55). Washington, 2003.

[So00] Soo Hoo, K. J.: How Much Is Enough? A Risk-Management Approach to Computer Security (Working Paper). Consortium for Research on Information Security Policy (CRISP), Stanford University, June 2000.

[SY05] Symantec: Symantec Internet Security Threat Report, Trends for July 04–December 04, 2005.

[We05] Weiß, S.: Metric for IT security in an organization. Diploma Thesis, University of Erlangen-Nuremberg, Department for Computer Sciences, Chair of Computer Science 7, 2005.