IT Security Certification and Criteria

Progress, Problems and Perspectives

KAI RANNENBERG
Microsoft Research Cambridge, UK
St. George House, 1 Guildhall Street, GB Cambridge CB2 3NH
kair@microsoft.com
www.research.microsoft.com/users/kair
www.iig.uni-freiburg.de/~kara

Key words: IT Security Certification, Evaluation, Criteria, Functionality, Assurance

Abstract: IT security certification and IT security evaluation criteria have changed their character compared with the first efforts ca. 20 years ago. They have also gained more interest within civilian and commercial application areas. Therefore this paper compares them with earlier criticism and with the new challenges in IT security. After an introduction into the concept of security certification the established IT security certification schemes and the related criteria are presented. Then their weaknesses and problems are described, in particular with regard to nowadays security requirements. Improvements of the criteria and the certification systems are presented, and suggestions for using current certification and evaluation schemes despite their shortcomings are made.

1. INTRODUCTION

IT security certification and its criteria are increasingly aiming at civilian and commercial security interests, and they got some relevance there: for example the German Digital Signature Act [6] asks for security certification of signature equipment and CA facilities. Also the landscape of organisations evaluating and certifying products and systems has changed; and new evaluation criteria (i.e. the "Common Criteria" [1] and the ISO/IEC Standard 15408 "Evaluation Criteria for IT Security" [9]) have been published. However, the certification schemes and criteria have always been subject to controversial discussions. Reasons were e.g. the weaknesses of the underlying security models, which impair the value of the evaluation results, and the high costs of certifications. It seems useful to present the current landscape of IT security certification schemes and criteria and check how far they have overcome earlier weaknesses.

S. Qing et al. (eds.), *Information Security for Global Information Infrastructures*

2. IT SECURITY CERTIFICATION

The complexity of today's IT makes it impossible to evaluate its security by simple "examination". However, users can hardly conduct the more detailed checks necessary for a qualified evaluation, as they cannot afford the costs. Thus, users are faced with the problem of knowing very little about the IT they use for important transactions, e.g. processing sensitive data, signing documents, or making payments. An approach to solve this problem is evaluation by independent test laboratories. Users can then refer to the evaluation results and don't depend solely on information from the vendors. They can also compare the evaluations to gain a market overview.

2.1 What is evaluated and certified?

Recent criteria differentiate two types of *Targets of Evaluation* (TOEs), i.e. *products* and *systems*. A *product* is defined as "a package of IT software and/or hardware, providing functionality, designed for use or incorporation within a multiplicity of systems". This means, in particular, that the operational environment of a product is not known during the evaluation. A *system* is defined as "a specific IT installation with a particular purpose and operational environment". This means that information about the operational environment can be used for the risk analysis. Additionally, the term "system" is often used for combinations of products.

There is only little public information on the evaluation and certification of systems, as this is rather expensive and has usually only been done for military applications. There are, however, a number of evaluated products:

- Chip card readers (ca. 43).
- Security products for PCs, including virus scanners (ca. 15).
- Products to protect data communication and network access (ca. 10).
- Operating systems for computers from mainframes to chip cards (ca. 18).

The numbers refer to certifications in Germany from 1991 to 1999 [5]. In the USA and the UK more products have been evaluated, especially operating systems and data base systems. The number of certifications may rise as a result of the German Digital Signature Act [6, §14(4)]. It mandates certification of equipment for digital signatures and public key infrastructures.

2.2 Evaluation, Certification, and Accreditation

In the context of IT security certification *Evaluation*, *Certification*, and *Accreditation* have a well-defined meaning and relation. It is best described by the terminology of the harmonized European IT Security Evaluation Criteria (ITSEC) [3]. They define *Evaluation* as "the assessment of an IT system or product against defined evaluation criteria". *Certification* is "the issue of a formal statement confirming the results of an evaluation, and that the evaluation criteria used were applied correctly". *Accreditation* has two definitions depending on the circumstances: "the procedure for accepting an IT system for use within a particular environment", or "the procedure for recognizing both the technical competence and impartiality of a test laboratory to carry out its associated tasks".

Evaluation and certification begin with the request of a *sponsor*, who is also responsible for the costs. Usually the sponsor is the manufacturer or developer of the TOE, it can also be any other vendor. The sponsor either applies directly to a Certification Body (CB) or contracts a test laboratory (*IT Security Evaluation Facility* – ITSEF) beforehand. The ITSEF advises the sponsor about the TOE, the security requirements (*Security Target* – ST) and the planned evaluation result, since most criteria leave these up to the sponsors' discretion. Often sponsors ask for the evaluation of only a part of the product, thus limiting the TOE, and also select only a limited ST.

The evaluation can take several months or years and is monitored by the CB. The ITSEF reports to the CB and to the sponsor. If the evaluation report is positive (and if there are no other facts known to the CB that contradict the report) the CB issues the certificate. The certificate is published with a certification report – if the sponsor agrees. Applications for certification can be made at all phases of the product life cycle; however, experience with the evaluation of products indicates that it is advisable to evaluate in parallel with development. Altogether, a certification can cost between ca. 50,000 and several million Euro, in particular, if the working time of the sponsor's personnel is taken into consideration.

The accreditation of an ITSEF is done by the accreditation body (sometimes identical to the CB) and repeated regularly (about every 5 years).

Originally, only government authorities certified and evaluated. They were usually offices in the area of defence or national security, e.g. in AUS, CDN, UK, USA. Later, the ministries of economic affairs or their offices (UK, USA), or the offices of the prime ministers (F, I), got involved. The UK and Germany were the first to have private companies as ITSEFs (other countries, e.g. the USA, have followed), and in Germany there are currently also private CBs.

The German certification scheme currently has the most options. The first CB was the German Information Security Agency (GISA), an office of the Ministry of the Interior. GISA also evaluates products and systems and accredits ITSEFs. Ca. 10 ITSEFs are accredited. After some criticism regarding this scheme and its inflexibility, the evaluation of components for digital signatures according to the Digital Signature Act [6] was organized differently: The Regulatory Authority for Telecommunications and Posts (RegTP; an office of the Ministry of Economics and Technology) recognizes CBs. In the meantime, GISA has contracts with three private CBs (all were accredited ITSEFs already) and, at the same time, RegTP has recognized these CBs and GISA.

2.3 Who uses Certificates for what?

Manufacturers and vendors, users and procurers, ITSEFs and CBs have different interests regarding certificates.

Manufacturers use certification mainly for the evaluation of products. Maintaining their image and promoting sales are often at least as important as the independent test of the product. The manufacturer of the first certified PC product in Germany offered both the certified version and a more advanced one with a higher version number, as both versions had their market. The certified version was mainly ordered by customers in public administration. Although certificates were not mandatory in that sphere, their existence influenced some decisions. The company also used the certification to document its position as "market leader".

Users and **procurers** initiated the idea of certification. At first, however, it was one particular group of users, i.e. the military of the USA that hoped to ease its procurers' work. At the same time, it wanted to structure the security requirements of its applications as simply as possible, in order to save the procurers from having to cope with details. This intention was encouraged by the assumption, that security requirements could simply be mapped onto a linear hierarchy. Moreover, as a special user group, the military had the buying power to mandate criteria to manufacturers.

For civilian users and private persons it is less easy to obtain similar benefits. Their security requirements, e.g. for enterprise information systems, are not structured that simply, and they are often not equipped with buying power comparable to that of the military. In this respect, the newer criteria are more helpful for civilian users and private people. These criteria are more evaluation criteria than security criteria and form a framework, within which "smaller" users can formulate their requirements – at least to a certain degree. An example of a user organization that requires certificates for certain products is the German National Association of Statutory Health Insurance Physicians. Also service providers, e.g. the Advance Bank, advertise the fact that their system for Internet banking has been certified. It is conceivable that insurance companies will mandate the use of certified products as a prerequisite for better contract conditions. Supervisory authorities (privacy protection commissioners) or employee representatives could require the use of certified products. Consumer federations could base their recommendations on certificates to simplify the selection of products or providers.

For **evaluation bodies**, certification is a competitive market. The volume of an evaluation can be below 10,000 Euro, but can also reach a million Euro. For the private **CBs** and their employees, certification means business and income, for the government **CBs** it is their legal task.

2.4 The Evaluation Criteria and who writes them

In 1983, the first criteria, the "Trusted Computer System Evaluation Criteria" (TCSEC) [14] were published. The rather protectionist certification policy of the USA, as well as the deficits of the TCSEC, which "prescribed" a very strict military view of IT security, made Europe and Canada develop own evaluation criteria (cf. Table 1).

Criteria from Germany (ZSISC [7]), France, and the UK were harmonized into the European ITSEC Version 1.2 [3]. In Canada, three versions of the CTCPEC [2] were developed, which had less and less similarity to the TCSEC. The ITSEC initiated the shift from the concept of "security criteria", which more or less defined IT security, to the concept of "evaluation criteria", which offer a framework to assist in describing the security characteristics that are to be evaluated. The ITSEC also served as a starting point for international standardization of the "Evaluation Criteria for IT Security" (ECITS, IS 15408, [9]) in a joint committee of ISO and IEC. This aimed at uniform criteria and mutual acknowledgement of evaluation results. Also the CTCPEC V. 3.0 influenced the ECITS. Parallel to the ISO/IEC standardization, North American and European government agencies are developing the "Common Criteria" (CC). CC Version 2.1 [1] and ECITS are fully aligned. At the moment there are no plans for another CC version, but the ECITS will undergo the usual periodic revision of ISO/IEC standards that will probably be done by JTC1/SC27 in 2003.

Table 1. IT security evaluation criteria and their editors

Publication / Project Dates	Editors	Criteria Name Current Version
1983/85	USA Department of Defense (DoD)	Trusted Computer System Evaluation Criteria (TCSEC) "Orange Book"
1989	Federal Republic of Germany (D) German Information Security Agency (ZSI)	IT-Security Criteria (ZSISC) Version 1
1990/91	Commission of the European Communities (CEC)	Information Technology Security Evaluation Criteria (ITSEC) Version 1.2
1990/93	Canada (CDN) Communications Security Establishment Canadian System Security Center (CSE/CSSC)	Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) Version 3.0
1990 - 99 2003?	International Organization for Standardization / International Electrotechnical Commission ISO/IEC JTC1/SC27/WG3	Evaluation Criteria for IT Security (ECITS) International Standard 15408 1999-12-01
1993 - 99	Common Criteria Project Canada / European Union / USA since 1994 CDN / D / F / UK / USA since 1995 CDN / D / F / NL / UK / USA since 10.1999 AUS / CDN / D / F / NL / NZ / UK / USA	Common Criteria (CC) Version 1.0 January 1996 Version 2.1 August 1999

2.5 Structure of the Criteria and Evaluation Results

Since the ZSISC and ITSEC all evaluation criteria divide security into two aspects: *Functionality* and *Assurance*:

1. *Functionality* covers what the TOE does, or can do, for security, e.g. measures for confidentiality, integrity, availability, and accountability.
2. *Assurance* covers the measures to produce the TOE in a secure way, and it covers the thoroughness of the evaluation. Assurance has two aspects:
   2.1. The evaluation of the *effectiveness* examines whether the functions and mechanisms of the TOE that implement security are really sufficient for the formulated objectives. Additionally, the strength of the security mechanisms against direct attacks is checked.
   2.2. The evaluation of the correctness examines whether the security functions and mechanisms of the TOE were implemented correctly.

Most evaluations produce a threefold result indicated in the certificate:

1. A description of the evaluated functionality.
2. An *evaluation level.* This level results, in particular, from the evaluation of the correctness and, partially, also from the evaluation of the effectiveness.
3. A classification of the *strength of mechanisms* of the TOE.

Each new criteria allowed more flexibility to describe the properties of a TOE, but on the other hand, made the comparison of evaluation results more complicated. In order to resolve this problem and to give users the opportunity to formulate their own requirements, the CC introduced the concept of *Protection Profiles* (PPs). A PP describes the functionality and assurance requirements for a certain application or technique. Ideally, several products will be evaluated against a PP and, as a result, can be compared.

3. CRITERIA AND CERTIFICATION PROBLEMS

The criteria caught much criticism for being too biased towards hierarchically administered technology, where the interests of the operators predominate those of the users. E.g. decentrally organized TOEs aiming at multilateral security [12] are only insufficiently covered. There was also no consideration of the fact that threats are caused not only by users and outsiders, but also by operators and manufacturers. Data collecting functionality was overemphasized, while data economical functionality was ignored. This is a problem as functionality not included in the criteria can hardly be recognized in certificates even if one is allowed to include it into the ST.

The following example illustrates how the lack of consideration for user protection in the criteria affects evaluation results. It also shows that the evaluation that is described was focussed on the protection of the operators and neglected the protection of users or customers. A function for the selective logging of activities of ***individual*** users was classified as a non-critical mechanism that did not need evaluation. In the opinion of the evaluators, failure of this mechanism would not create weaknesses because if the function was not active, the activities of all users were logged [4]. From the operator point of view no real security risk existed, because no audit data would be lost – only perhaps more data than planned would be collected. However, excessive logging and the resulting data can lead to substantial dangers for users and customers.

The newer criteria (e.g. CC 2.x or ISO ECITS) have overcome many weaknesses of their predecessors, but they are still restricted in their suitability for formulating the requirements of multilateral security. There has been substantial progress, e.g. the unobservability of communications is covered by some criteria components, but these passages are very short, while material from the TCSEC, e.g. regarding "audit" occupies a much larger part of the document.

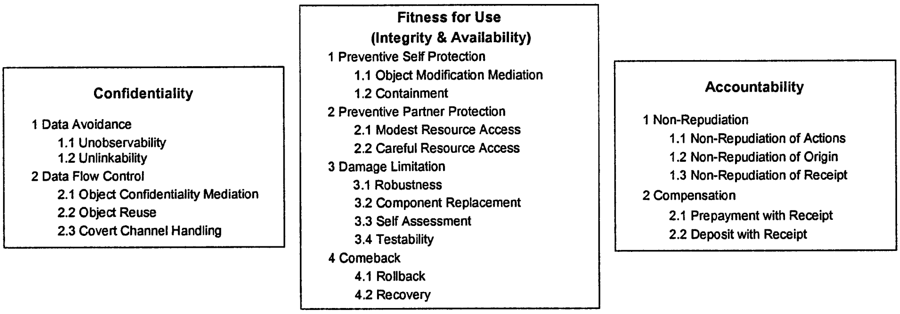
Other aspects of security certification and the underlying criteria that have been criticized are:

- The **certification schemes**: Many users have not viewed the quasi government monopoly of CBs as being trustworthy enough. Some applicants also considered the government CBs insufficiently flexible to get a product through certification and on the market as quickly as they wanted.
- The meaningfulness and the use of the **results**: A high evaluation level, e.g. E4, or the mere fact that a certification took place, don't necessarily mean a general high degree of security. PR departments however tend to create the impression of "totally checked security", and customers have a problem, if they don't know, which part of the product was evaluated according to which requirements – and which part was not.

- The **lack of certified products**: If users insisted on only using certified products, they would have to do without most standard application software, in many cases, even without an operating system.
- The **costs** of certification: It does not encourage sponsors, if the costs of certification exceed the revenue that can be expected from the product. However, sponsors usually don't complain too much about the CBs' fees or the ITSEFs' costs, but rather about the costs for personnel on their part, particularly as certifications have often taken longer than expected.
- The **criteria editing process**: The writing and interpreting of the governmental criteria was neither controllable, nor comprehensible for interested experts – only the ISO committee was a rather open editing group.

4. A NEW STRUCTURE FOR SECURITY FUNCTIONALITY IN CRITERIA

The structure, which is briefly presented here, aims at covering to the best extent possible all functionality necessary for security, without becoming too detailed. For this reason 3 levels were selected (cf. Fig. 1): "Security" is divided into 3 *targets* (level 1). These targets can be implemented by the correct combination of functionality from altogether 20 *functional building blocks* (level 3), which are grouped into 8 *protection principles* (level 2).



Confidentiality

1 Data Avoidance
- 1.1 Unobservability
- 1.2 Unlinkability

2 Data Flow Control
- 2.1 Object Confidentiality Mediation
- 2.2 Object Reuse
- 2.3 Covert Channel Handling

Fitness for Use
(Integrity & Availability)

1 Preventive Self Protection
- 1.1 Object Modification Mediation
- 1.2 Containment

2 Preventive Partner Protection
- 2.1 Modest Resource Access
- 2.2 Careful Resource Access

3 Damage Limitation
- 3.1 Robustness
- 3.2 Component Replacement
- 3.3 Self Assessment
- 3.4 Testability

4 Comeback
- 4.1 Rollback
- 4.2 Recovery

Accountability

1 Non-Repudiation
- 1.1 Non-Repudiation of Actions
- 1.2 Non-Repudiation of Origin
- 1.3 Non-Repudiation of Receipt

2 Compensation
- 2.1 Prepayment with Receipt
- 2.2 Deposit with Receipt

Figure 1. Structuring security functionality into 3 goals, 8 protection principles and 20 functional building blocks

The following motives determined the detailed organization of the structure:

1. Functionality of IT that can be evaluated is represented. Accordingly, the functional building blocks are mainly measure-oriented, while the targets are all property-oriented. A structure, that is oriented exclusively towards the characteristics of information, could look different, cf. e.g. [10].
2. In the interest of clarity, the number of functional building blocks was kept as low as possible. An independent functional building block was selected if one *has to* react to special characteristics of IT and one *can* react with IT measures. On the other hand, the functional building blocks were made just broad enough to allow them to be distinguished according to hierarchical levels.

Starting point for the structure was the functionality taken from the ISO ECITS in their version of Winter 1995/96 [8], which is partially based on the CTCPEC [2]. The ISO ECITS functionality was restructured, parts were summarized and parts were expressed in more detail. Further meaningful functionality resulted from the systematic of the new structure. A detailed analysis and allocation of the functions can be found in [11], together with the application of the new structure to the security functionality of an ISDN Private Automatic Branch Exchange (PABX).

5. IMPROVING THE ORGANISATION

Criteria alone do not automatically lead to expressive and useful certificates. It is equally important to have an appropriate organization of the following areas:

1. Certification.
2. Evaluation.
3. Accreditation of the ITSEFs.
4. Information and consultation for non-insiders.
5. Further development and maintenance of criteria and methods.

The following two sections briefly present requirements for areas 1 and 5.

5.1 Organization of Certification

As long as the criteria are imperfect, the ITSEFs, the accreditation bodies, and particularly the CBs have a special responsibility, but even if there were perfect criteria the following requirements would still be important:

1. Flexible handling of what the existing criteria mean by "Security". The evaluation of TOEs, which contain functionality not (yet) covered by the criteria, should not suffer as a result of this deficit of criteria.
2. Continuous monitoring of certificate validity. This can mean a re-evaluation, if the basic conditions of the certification have changed, e.g. if mechanisms have been compromised. It can also mean the temporal limitation of certificates.
3. Decentralized organization and real public control over not only the evaluation bodies, but also the accreditation and CBs.
4. An internationally organized public evaluation of cryptographic mechanisms.

A step towards more transparency can be taken with the establishment of additional private CBs. This alone neither solves problems, nor has to be the solution.

5.2 Organization of the Criteria Development Process

Experience with IT security evaluation criteria has shown that, after a few years at the latest, some of the assumptions which were used as a basis for the criteria are outdated. So far, the necessary revisions occurred as different nations successively developed criteria. Now, after the criteria are harmonized, they need a reliable revision process. Comparing different approaches, e.g. the ISO/IEC standardization and the closed committees of the CBs, and considering the experience gained from criteria development and harmonization, one comes to a, perhaps surprising, conclusion: ISO/IEC standardization, much-scolded for its alleged tardiness, but with its nevertheless comparatively open approach, offers the best conditions for the development of IT security evaluation criteria. A reason for this may be that evaluation criteria place less emphasis on technical details, and more on a guiding framework and structure. The main reason is probably that the participation of as many interested parties as possible is particularly important.

6. HOW TO USE EVALUATIONS AND CERTIFICATES DESPITE THEIR SHORTCOMINGS

The criteria, as well as the organization of certification, need improvement, but the existing scheme and the available certificates can also be used meaningfully, if their weaknesses are taken into account. In respect of certificates the following points need to be considered:

1. No certified TOE can guarantee absolute security or eliminate the need to personally conduct risk analysis and develop a security concept.
2. The purpose of certificates is not to believe in them, but to read them. In particular, the certification reports that, are often available on the WWW pages of the CBs, contain much more information than a simple evaluation level. They are also a helpful basis for discussions with vendors.
3. One has to consider not only what was evaluated, but also what was *not* evaluated. Often the networking components have been excluded from the evaluation, in order to limit complexity and costs.
4. The TOE, the ST, and the evaluation level, are determined by the sponsor. Accordingly, the ST is often adapted to the strengths of the TOE and the evaluation level is adapted to what the sponsor is willing to pay.

If one **operates** a system and wants to fulfil internal requirements or needs support with accreditation, then an evaluation without a formal certificate [13] delivers an independent judgement at lower costs. **Users** looking for support in the selection of a system or products should consider formulating a PP – even if this is only to structure their own requirements. In addition, it is advisable to keep an eye on the increasing number of PPs.

Sponsors should consult an experienced ITSEF before going for a certification, to learn as early as possible about the evaluation requirements, especially regarding documentation. Evaluating in parallel to development can save much time and also raises the chance to have a certificate when the product is introduced to the market.

7. CONCLUSION AND OUTLOOK

In principle, the concept of IT security certification has many strengths, however, in its present state there are still substantial weaknesses. The structure for security functionality, presented briefly in this text, overcomes deficits and structural weaknesses of the earlier evaluation criteria. It is probably not the final applicable structure, but it is a step towards taking the requirements of multilateral security into account. However, there are still things that need to be accomplished, for example, in the following areas:

1. Further development of the criteria will continue to be necessary. Via ISO it was possible to integrate some essential elements of multilateral security into the Version 2.x of the CC, which makes it, to a certain extent, complete. The structure of functionality in the CC is, however, virtually non-existent, due to the fact that a consistent structure for the classification of functional components was, in the end, less important than consensus among the developers.
2. An acid test for the criteria will be using them for innovative TOEs, e.g. signature equipment or devices, which help users to protect their personal data. As a prerequisite for this, specific interpretations of the criteria, e.g. PPs have to be formulated. Their formulation will show whether the functional components of the criteria are adequate.
3. Results have to be made accessible for users in an understandable form.

In addition, it will be worthwhile to investigate the evaluation and certification of whole systems more thoroughly. There is also a need to lower the costs for evaluation and certification, e.g. by more integration into the manufacturers' development and quality assurance processes.

REFERENCES

[1] Common Criteria Implementation Board: Common Criteria for IT Security Evaluation, V. 2.1, August 1999; http://csrc.nist.gov/cc

[2] Canadian System Security Centre: The Canadian Trusted Computer Product Evaluation Criteria, V. 3.0e; Jan. 1993

[3] European Commission: IT Security Evaluation Criteria, V. 1.2; 1991-06-28; Office for Official Publications of the EC; also www.itsec.gov.uk/docs/pdfs/formal/ITSEC.PDF

[4] C. Corbett: ITSEC in Operation – an Evaluation Experience, Proc. 4th Annual Canadian Computer Security Conference, May 1992, Ottawa, Canada, pp. 439-460

[5] Bundesamt für Sicherheit in der Informationstechnik: German IT Security Certificates; BSI 7148E; September 1999; www.bsi.de/aufgaben/ii/zert

[6] Deutscher Bundestag: Gesetz zur digitalen Signatur vom 22. 7. 1997; Bundesgesetzblatt I, S. 1870; in english www.iid.de/rahmen/iukdgebt.html

[7] German Information Security Agency: IT-Security Criteria, Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems; Jan. 1989, Bundesanzeiger

[8] ISO/IEC JTC1/SC27: Evaluation Criteria for IT Security, Part 1-3, Working Drafts 1995-12-15; ISO/IEC JTC1/SC27/N1269-71

[9] Evaluation Criteria for IT Security, Parts 1-3; International Standard 15408; 1999-12-01

[10] D. Parker: A new Framework for Information Security to avoid Information Anarchy; in J. Eloff, S. v. Solms: Proc. TC11 11th Int. Conf. on Inform. Security; Chapman & Hall

[11] K. Rannenberg: Zertifizierung mehrseitiger IT-Sicherheit – Kriterien und organisatorische Rahmenbedingungen; Vieweg

[12] K. Rannenberg, A. Pfitzmann, G. Müller: IT Security and Multilateral Security; in G. Müller, K. Rannenberg: Multilateral Security in Communications – Technology, Infrastructure, Economy; Addison-Wesley-Longman, 1999; ISBN 3-8273-1360-0

[13] R. Schützig: Prüfung und Zertifizierung von IT-Installationen; Datenschutz und Datensicherheit, Vol. 22(4), pp. 207-210

[14] Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html