pp. 113-128 in: "SECURITY AND CONTROL OF INFORMATION TECHNOLOGY IN SOCIETY – Proceedings of the IFIP TC9/WG 9.6 Working Conference August 12-17, 1993, onboard M/S Ilich and ashore at St. Petersburg, Russia" edited by Richard Sizer, Louise Yngström, Henrik Kaspersen and Simone Fischer-Hübner; published by North-Holland, Amsterdam 1994

Recent Development in Information Technology Security Evaluation – The Need for Evaluation Criteria for multilateral Security

Kai Rannenberg

Department for Telematics, Institute for Informatics and Society, University of Freiburg
Friedrichstraße 50, D-79098 Freiburg, Germany
Phone +49-761-203-4926, Fax +49-761-203-4929, E-Mail kara@iig.uni-freiburg.de

More and more the security of information technology becomes subject to evaluations by neutral third parties beside manufacturers and procurers. The basis of these evaluations are information technology security evaluation criteria. This contribution reports and analyses the recent development of national and harmonised criteria and the development in the international standardisation, especially in the relevant committees of ISO and IEC. General trends like the distinction between "Security Functionality" and "Assurance", the liberalization in the description of security functionality and the need for multilaterally secure information technology are described and commented on. The development of "Security Functionality" towards a broader but still not comprehensive scope is documented by an analysis of the structural entities "Facets of Security" and "Generic Headings to specify security functionality" and their mutual relationships. Based on recent development in ISO standardisation a proposal for a structure of security functionality covering multilateral security is presented. In conclusion the most important requirements on security evaluation criteria and certification schemes are summarized and their significance for the new countries in eastern Europe is discussed.

Keyword Codes: K.7.3; K.6.5; D.4.6
Keywords: The Computing Profession, Certification, and Licensing; Management of Computing and Information Systems, Security and Protection; Operating Systems, Security and Protection

0 INTRODUCTION

Complexity of information technology (IT) makes it more and more difficult for procurers to decide whether offered systems fulfill their requirements. This is especially true in the field of IT security. Therefore in the late 70es government initiatives were started to establish schemes, especially criteria catalogues and evaluation facilities, for the security evaluation and certification of IT products and systems by – hopefully – neutral third parties.

Security can be evaluated within special systems operating in a known environment, e.g. military information systems, as well as within products, which may be produced for a mass market, e.g. personal computer security tools. Certificates are issued by national agencies, which might delegate the evaluation and the authorship of evaluation reports to accredited test

houses (Commercially Licensed Evaluation Facilities). Costs of evaluations are to be paid by the sponsors of the evaluation, which in most cases are the manufacturers of the evaluated IT products or systems.

Although there is legitimate fundamental criticism on the general insecurity of today's IT systems and the inappropriate metrical approach of current evaluation criteria [Brunnstein, Fischer-Hübner 1990, 1992] today's procurers, especially in the public administration, need help in the analysis of today's market alternatives in respect to the requirements of their sensitive information processing facilities. Third-party evaluation and certification seems to be a helpful instrument, and evaluation criteria are a way to raise the comparability of security certificates.

On the other side the bias of current evaluation criteria towards a functionality providing security only for system owners and operators causes severe risks for individuals and the whole of society. The same is true for assurance methods being biased to formal specifications while neglecting the risks of development tools [Gehrke, Pfitzmann, Rannenberg 1992]. The risks are raised as standards often tend to establish the current state of the art forever. This makes it difficult to consider new developments, e.g. the rising need and demand for multilateral security, which cover the requirements of users and usees as well as those of IT system owners and operators. In consequence the international development of IT security evaluation criteria needs attention not only by experts of "classical" IT security.

While there are international public statements proclaiming international agreement on the fast harmonisation of the several evaluation criteria and certification schemes to reach mutual recognition of certificates and save costs for industry, the international development is not only driven by the endeavour for unified criteria of high quality, but also by the preservation of national competitiveness and company interests. Therefore this contribution describes and comments the international development of evaluation criteria for IT security considering non-technical factors as well as technical ones.

The national and regional criteria together with the international standardisation activities, especially in the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC), are introduced in Chapter 1. Chapter 2 reports and analyses general trends in the development of IT security evaluation criteria, such as the distinction between "Security Functionality" and "Assurance", the liberalization in the description of security functionality, and the need for multilaterally secure IT. The development of "Security Functionality" towards a broader but still not comprehensive scope is described and documented by an analysis of the structural entities "Facets of Security" and "Generic Headings to specify security functionality" as well as their mutual relationships in Chapter 3. Additionally a proposal for the structure of security functionality covering multilateral IT security and based on recent developments in ISO standardisation is presented. The concluding Chapter 4 summarizes the most important requirements on IT security evaluation criteria and certification schemes and discusses their significance for the new countries in eastern Europe.

1 THE NATIONAL AND INTERNATIONALLY HARMONIZED CRITERIA

While the USA started the development of criteria for IT security evaluation this is done worldwide now. This chapter presents a short introduction to the US-American (1.1, 1.5),

European (1.2), Canadian (1.3), Japanese (1.4) and international (1.6) initiatives and documents.

1.1 The TCSEC of the United States Department of Defense

1983 the Department of Defense of the USA published the "Trusted Computer System Evaluation Criteria" (TCSEC) for the first time, 1985 a second version with only minor changes followed [US_DOD 1983, 1985]. Their popular name "Orange Book" corresponds to their cover pages colour. Four security divisions and 7 classes reach from division D (minimal protection) to class A1 (verified design) in division A (verified protection). The TCSEC are focussed on the security requirements of classified document handling applications based on mainframe computer systems. Interpretations of the TCSEC have been published to apply them to other techniques, e.g. the "Trusted Network Interpretation of the TCSEC" [US_NCSC 1987]. Despite discussions on new U.S. criteria (cf. 1.5) the TCSEC still are the basis for security evaluations in the United States.

1.2 The ITSEC of the Commission of the European Communities

Developments in IT and the U.S. evaluation policy concerning non-U.S. companies made several European countries develop own criteria and evaluation schemes. The Commission of the European Communities (CEC) harmonised them into the "Information Technology Security Evaluation Criteria" with a first version 1.0 being published in 1990 [CEC_1990] mainly based on the following national criteria documents:

- The French Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information [SCSSI 1989];
- The British UK Systems Security Confidence Levels [CESG 1989];
- The British DTI Commercial Computer Security Centre Evaluation Manual [DTI 1989_1];
- The British DTI Commercial Computer Security Centre Functionality Manual [DTI 1989_2];
- The German IT-Security Criteria (ZSIEC) [GISA 1989].

Additionally, the Netherlands contributed to ITSEC. Though major weaknesses (cf. 3.2 and [Rihaczek 1991; GI 1992; Gehrke, Pfitzmann, Rannenberg 1992]) of ITSEC V1.0 were not eliminated in version 1.2 published in June 1991 [CEC_1991], this version became a basis for evaluations in the CEC member states at least for a two year trial period. As there is no consensus on the official beginning of that trial period, the publication of a version 2.0 of ITSEC is unclear, but not expected to happen in 1993.

1.3 The CTCPEC of the Canadian System Security Centre

In August 1988, the Canadian System Security Centre (CSSC) at the Communications Security Establishment of the Government of Canada was formed to develop a set of criteria and to set up a Canadian evaluation capability among other tasks. In April 1992 a draft of version 3.0 of "The Canadian Trusted Computer Product Evaluation Criteria" (CTCPEC) was published [CSSC 1992]. It can be seen as a further development beyond the scope of the TCSEC and the ITSEC, and its approach to structure security functionality influenced international standardisation (cf. 3.3 and 3.5). In January 1993 the final version of CTCPEC version 3.0 [CSSC 1993] was published.

1.4 The JCSEC-FR of the Japan Electronic Industry Development Association

In August 1992 the Japan Electronic Industry Development Association (JEIDA), a non-profit organisation formed by Japanese electronics manufacturers, published version 1.0 of the "Japanese Computer Security Evaluation Criteria – Functionality Requirements" (JCSEC-FR) for review purpose [JEIDA 1992]. The document is aligned very much with the functionality part of the ITSEC but specified in greater detail. A second document on assurance requirements is announced to follow.

1.5 The FC-ITS of the United States NIST and NSA

Following the international discussion and trying to meet also the needs of non-military, especially commercial IT applications the U.S. launched a project to produce a TCSEC successor (cf. 1.1). A first document were the "Minimum Security Requirements for Multi-User Operating Systems" published by the Computer Security Division of the Computer Systems Laboratory at the National Institute of Standards and Technology (NIST) [USA_NIST 1992], which present security functionality requirements for operating systems processing non-classified information in a governmental and commercialenvironment.

In December 1992 the draft version 1.0 of the "Federal Criteria for Information Technology Security" (FC-ITS) was published by NIST and the National Security Agency (NSA) for review and discussion [US_NIST_NSA 1992]. This document is planned to evolve into a new U.S. Federal Information Processing Standard (FIPS) "intended principally for the use by the U.S. Federal Government, and also by others as desired and appropriate". A second version is announced for October 1993, and further versions are intended to be harmonised on a North American and transatlantic basis.

1.6 International Standardisation and Harmonisation

In October 1990 the Joint Technical Committee 1 of the International Organisation for Standardisation and the International Electrotechnical Commission (ISO/IEC JTC1) established Project 1.27.16 "Evaluation Criteria for IT Security" in Working Group 3 "Security Evaluation Criteria" of Subcommittee 27 "Security Techniques" (SC27/WG3). The new standard is intended to have three parts:

(1) Part 1 "General Model of Security Evaluation": Svein Knapskog (University of Trondheim, Norway), Convener of SC27/WG3, served as editor, until in October 1992 Eugene Troy (NIST, USA) took over.

(2) Part 2 "Functionality of IT Systems, Products and Components": Michael Nash (Gamma Secure Systems Ltd., UK) serves as editor.

(3) Part 3 "Assurance of IT Systems, Products and Components": Markus Wagner (TÜV Bavaria, Germany) served as editor until March 1993. Ulrich van Essen (German Information Security Agency) is recommended by WG3 to SC27 as new editor.

The project is divided along the structure of the ITSEC, which served as textual input for the first working drafts (WD) of part 2 and 3. Additionally to problems in the harmonisation of terminology and to the ITSEC weaknesses (cf. 1.2 and 3.2) the absence of USA comments on the working drafts slowed down the standardisation process: No part of the standard has been

forwarded to Committee Draft (CD) level, the second of four levels on the way to an ISO/IEC International Standard. The current status of the documents shows great differences between the three parts, especially between part 1, which tends into the direction of the FC-ITS and part 3, which still has strong similarity to the ITSEC approach. Part 2 has been influenced by the CTCPEC (cf. 3.3 and 3.5).

Additionally a project on the "Collection and analysis of requirements for IT security evaluation criteria" has been set up, but due to the lack of a project editor progress is slow. A new project for the registration of functionality classes is out for ballot by national standardisation bodies (cf. 2.4). Technical Committee 36 of the European Copmputer Manufacturers Association (ECMA) is developing an example functionality class for commercial purposes [ECMA 1993].

Considering the slow progress in ISO/IEC European countries are thinking about establishing the ITSEC as a European standard within the European Committee for Standardisation (CEN). Further actions in this area might depend on the success of joint Canadian, European and U.S. government task forces on harmonisation of "Functionality", "Evaluation Methods" and "Common Criteria".

2 DEVELOPMENT OF IDEAS AND CONCEPTS

The discussion on national and harmonised criteria catalogues published since the issue of the TCSEC introduced new ideas and concepts. Four of the main trends are:

(1) The distinction between functionality and quality aspects of IT security in the ITSEC and ISO/IEC documents (cf. 2.1),

(2) The treatment of dependencies between functionality and assurance as done in the CTCPEC and especially the FC-ITS (cf. 2.2),

(3) The deregulation of the meaning of security functionality as an overall trend (cf. 2.4);

(4) The rising need for a structure of security functionality covering multilateral security (cf. 2.5).

Problems in the – transatlantic – harmonisation of terminology are described in 2.3. A more detailed discussion of security functionality and its structure can be found in Chapter 3.

2.1 Distinction between Functionality and Assurance (ITSEC and CTCPEC)

The ITSEC and before them the ZSIEC introduced a distinction between two aspects of security: functionality and assurance:

(1) Functionality contains, what a system does to be secure, e.g. auditing of security relevant events or identification and authentication of users;

(2) Assurance contains, what developers and evaluators of the system did to ensure the security of the system, e.g. by formal verification or testing.

According to this distinction ITSEC certificates have two components. They are given for a certain functionality tohether with a certain assurance level between E0 and E6. An annex of the ITSEC contains 10 functionality classes, which are examples for combinations of certifiable functionality. 5 of them are derived from the TCSEC. After discussion the functionality classes

are not mandatory any more as they were in the German ZSIEC. As ITSEC certificates have two independent components there is no strict hierarchy of all types of certificates like in the TCSEC.

Beside a lot of criticism for several weaknesses (cf. 2.5 and 3.2) the distinction between functionality and assurance brought acknowledgement and applause to the ITSEC, as this distinction raised the transparency of certificates. At least officially there was no big discussion on the loss of the strict hierarchy of certificates, and ISO/IEC JTC1/SC27/WG3 divided its evaluation criteria project in accordance with the ITSEC structure (cf. 1.6). Also the Canadian CTCPEC follow this dual approach.

2.2 Functionality and Assurance Dependencies (FC-ITS and CTCPEC)

Despite the acknowledgement for the distinction between functionality and assurance aspects of IT security, there exist phenomena of risks and security mechanisms, which show dependencies between functionality and assurance.

One example is the problem of covert channels – channels where information can flow around the barriers of a given security policy. Covert channel handling is a functionality aspect of security, covert channel analysis is a part of assurance. Cutting the two aspects from each other can produce a security hole, if analysis and handling do not match. Another example is the evaluation of mechanisms for identification and authentication: testing of mechanisms, which allow users to choose and administrate passwords by themselves, differs from testing of mechanisms, which use one-time password devices. "Do-it yourself" mechanisms must be tested e.g. for proper minimum password length, lifetime limitation for passwords and context complexity, while with password generating mechanisms the pseudo-random sequence generation must be tested by different means.

The FC-ITS contain separate chapters on "functionality" and "assurance" requirements, but introduce a new structure based on the aspect of dependencies between functionality and assurance. "Protection Profiles" are designed to cover fitting functionality and assurance requirements and to replace "Functionality Classes" and "Functionality Profiles".

Dependencies are also considered in the CTCPEC [CSSC 1992, p. 127; CSSC 1993, p.2] and documented by constraint relations between functionality and assurance aspects. However the CTCPEC authors did not let dependencies have a strong influence on the overall structure of the criteria document. Additionally the "Functional Profiles" of the CTCPEC define "Functionality" similar to the way the "Functionality Classes" of the ITSEC do.

The discussion on dependencies is going on: On one side the dependency issues might justify a restructuring of the criteria and the "Protection Profiles" might be helpful for users to specify their security needs. On the other side both ideas are suspected of just defending old structures deriving from the TCSEC and protecting the U.S. IT market, especially as 5 of the 7 example protection profiles in the FC-ITS were taken from the TCSEC security classes.

2.3 Problems in the Harmonisation of Terminology

Several problems complicate the international, especially the transatlantic harmonisation of criteria. The most striking example is the different meaning of the term "Certification" in Europe and the U.S. Certification in Europe means "the *issue of a formal statement* confirming the

results of an evaluation, and that the evaluation criteria used were applied correctly" [CEC 1991, p. 112]. The current draft of the FC-ITS defines certification as "Comprehensive evaluation of the technical and nontechnical security features of an automated information system and other safeguards, made in support of the accreditation process to establish the extent to which a particular design and implementation meets a set of specified security requirements" [US_NIST_NSA 1992, vol. 1, p. 203]. This definition is comparable to that of "Evaluation" in Europe. In consequence the term "Certification" can cause severe transatlantic misunderstanding, as in Europe it means the – by now in most cases successful – end of an evaluation, while in the U.S. it just says an evaluation is going on. As the FC-ITS definition contains the word "evaluation" there is evidence to prefer the European distinction, but the transatlantic Canadian, European and US-American task force set up for this – and other – work has not agreed yet.

2.4 Deregulation of the Meaning of Security Functionality

The TCSEC contain an implicit strict definition of security functionality (cf. 3.1) and assurance. TCSEC classes are ordered in a strict hierarchy following one goal. Some years later the ITSEC opened a way for sponsors (manufacturers) to choose their own target of evaluation by combining security functionality as they like. Even functionality classes are just examples – at least from an official point of view. This fact softens the discussion, which functionality classes are really needed.

The current status of the decisions in ISO/IEC JTC1/SC27/WG3 is to place examples of predefined functionality classes – ideally from different sources – into an informative annex of the "Functionality" part of the standard. To set up an entity for the vetting and administration of functionality classes currently a new work item on "Procedures for the creation of a restricted registry for functionality classes" is ballotted by the national standardisation bodies. AFNOR, the French national standardisation body, offered to serve as the registration authority. Nevertheless it is possible that the content of the registry will change from functionality classes to protection profiles (cf. 2.2).

The deregulation of the meaning of security functionality and the possibly decreasing importance of functionality classes raise the importance of models to structure and describe security functionality, as they are treated in Chapter 3.

2.5 The Need for multilaterally secure Security Functionality in Criteria

The TCSEC had a strong bias on the protection of system owners and operators only. This bias is slowly losing strength, but can still be seen in all criteria published afterwards. Security of users and usees, especially of users of telecommunication systems is not considered. Therefore techniques, providing bi- or multilateral security, e.g. those protecting users in a way privacy regulations demand it, cannot be described properly using the current criteria. This complicates the proper evaluation and certification of these techniques.

Examples for techniques providing multilateral security are MIX- and DC-Nets [Chaum 1985; Pfitzmann, Pfitzmann, Waidner 1991] which provide unobservability and unlinkability of communication events and by this means e.g. can help users to communicate anonymously and free from observation by system and network operators. Another set of examples are systems

allowing electronic value transfer without the danger of consumer profiles in the hands of banks and trading companies [Chaum 1985; Bürk, Pfitzmann 1990].

Especially the ITSEC caught hard criticism for their bias on the protection of the system owners and operators only [Brunnstein, Fischer-Hübner 1992; Gehrke, Pfitzmann, Rannenberg 1992]. Even a special task force of Gesellschaft für Informatik, the German IFIP full member, set up a strong set of comments [GI 1992]. Additionally there is the general demand, that evaluation criteria do not only meet technical issues, but also consider legal standards, legal conditions, environmental factors and ethics [Kaspersen 1992]. Chapter 3 gives a short analysis of all current criteria in respect to their structure of security functionality and their ability to integrate multilateral security functionality.

3 STRUCTURE AND DESCRIPTION OF SECURITY FUNCTIONALITY

During the years since the publication of the TCSEC the scope of "Security Functionality" has broadened considerably. In this chapter this development is described and documented by a description of the – in most criteria two - levels of structural entities to specify security functionality:

(1) Most abstract definitions are given by terms like "Meanings of Security" (ITSEC), "Functional Criteria" (CTCPEC), "Policy Components" (FC-ITS) or "Facets of Security" (ISO/IEC).

(2) More concrete definitions are given by terms like "Generic Headings to specify security functionality" (ITSEC), "Security Services" (CTCPEC, ISO/IEC) or "Functional Components" (FC-ITS).

Additionally the mutual relationships of the structural entities and their ability to cover multilateral security functionality are analyzed and worked out. As the JCSEC-FR structure functionality requirements in line with the "Generic Headings" of the ITSEC, they are covered by the Subchapter 3.2 on the ITSEC.

3.1 USA-TCSEC: Confidentiality

The TCSEC presented a very simple meaning of security functionality: Security was the confidentiality of the system owner's documents. Therefore the TCSEC do not contain a further structure of security functionality but merely a list of security mechanisms. Both might be a reason why only the first part of the Trusted Network Interpretation of the TCSEC [US_NCSC 1987] could be structured in accordance with the TCSEC with all major networking issues being treated in the second part.

3.2 CEC-ITSEC: Properties and Generic Headings

European criteria, as the ITSEC and their German predecessor ZSIEC, presented a broader range of security functionality than the TCSEC did and introduced a 2-layer-structure for the description of security functionality. On a first – more abstract – level there are three properties covering risks to information and resources, on a second level there are 8 "Generic Headings" for the description of security functionality. The ITSEC do not contain a matching between the three properties and the 8 generic headings. The three ITSEC properties of IT security are:

(1) Confidentiality: the prevention of the unauthorised disclosure of information;
(2) Integrity: the prevention of the unauthorised modification of information;
(3) Availability: the prevention of the unauthorised withholding of information or resources.

While confidentiality is aligned with the TCSEC, integrity and availability are additional properties. The 8 generic headings of the ITSEC are:

(1) Identification and Authentication
(2) Access Control
(3) Accountability
(4) Audit
(5) Object Reuse
(6) Accuracy
(7) Reliability of Service
(8) Data Exchange

The use of these generic headings is not strictly mandatory, but strongly recommended. They have been strongly criticised for being unsystematic and incomplete, as necessary duals to cover multilaterally secure security functionality are missing [Gehrke, Pfitzmann, Rannenberg 1992, GI 1992]. A way to integrate this functionality is the introduction of the duals "Anonymity and Pseudonymity" to "Identification and Authentication" and "Unobservability" to "Audit". However this addition can be only a provisional solution, and restructuring of the set of generic headings might be more fruitful (cf. 3.3 or 3.5).

3.3 Canada-CTCPEC: Functional Criteria and Services

Version 3.0 of the CTCPEC [CSSC 1993] presents another 2-layer-structure with four "Functional Criteria" as a the abstract structure. Each of the four "Functional Criteria" is divided into – altogether 18 – "Security Services" (cf. Table 1).

1 **Confidentiality**	Covert Channels Discretionary Confidentiality Mandatory Confidentiality Object Reuse
2 **Integrity**	Domain Integrity Discretionary Integrity Mandatory Integrity Physical Integrity Rollback Separation of Duties Self Testing
3 **Availability**	Containment Fault Tolerance Robustness Recovery
4 **Accountability**	Audit Identification and Authentication Trusted Path

Table 1: **Functional Criteria** and their divisions in the CTCPEC

There has been criticism (cf. 3.5) that this structure promotes mechanisms like self testing on the same level as security functionalities e.g. identification and authentication. Additionally – like the TCSEC and the ITSEC – the CTCPEC do not include multilaterally secure security functionality. Despite this the CTCPEC's fourfold structure of functional criteria at least gives proper room for the integration this functionality (cf. 3.5).

3.4 USA-FC-ITS: Taxonomy of TCB Functions

The FC-ITS present security functionality as a part of the functions of a trusted computing base (TCB) on three levels. The first level divides "Security Policy Support" from "Reference Mediation" and some functions to directly protect the TCB. Beside a "Security Management" section the "Security Policy Support" division contains three sections to structure security functionality in a way comparable to the other criteria. These three "Policy Components" and their "Functional Components" are given in table 2.

1 **Accountability Policy**	Identification and Authentication System Entry Trusted Path Audit
2 **Access Control Policy**	Discretionary Access Control Policies Non-Discretionary Access Control Policies Covert Channel Handling
3 **Availability Policy**	Resource Allocation Fault Tolerance

Table 2: **Security Policies** and their components in the FC-ITS

The functionality structure of the FC-ITS has some similarities to that of the CTCPEC, but even more to the TCSEC, which is said to be caused by NSA influence. Integrity as well as confidentiality are integrated into the component "Access Control Policy". The following are two ways to integrate multilateral security functionality into the current structure of FC-ITS:

(1) A new substructure "Privacy Policy" could be added to the security policy components.

(2) The meaning of "Access Control" could be broadened even further.

The first alternative seems to be the better one, if the current structure cannot be changed, but a complete restructuring might be even better. As the current – first – draft of the FC-ITS does not define all parts of the functionality completely, one can expect further changes in near future, e.g. from the second draft (cf. 1.5).

3.5 ISO/IEC JTC1/SC27/WG3: Facets and Services

International Standardisation in ISO/IEC JTC1/SC27/WG3 (*W*orking *G*roup 3 in *S*ub*c*ommittee 27 of the *J*oint *T*echnical *C*ommittee 1 of the *I*nternational *O*rganisation for *S*tandardisation and the *I*nternational *E*lectrotechnical *C*ommission, cf. 1.6) began with documents very similar to the ITSEC. After a long discussion on the suitability of the 8 ITSEC generic headings and their weaknesses, in October 1992 it was decided to accept a Canadian proposal very similar to the CTCPEC and to add multilateral security services to the Canadian proposal to include them after further discussion. The outcome was a structure with four "Facets of Security" and 19 "Security Services" as listed in table 3:

1 **Confidentiality**	Covert Channels Discretionary Access Control Mandatory Access Control Object Reuse Unobservability [additional to CTCPEC] Anonymity [additional to CTCPEC]
2 **Integrity**	Discretionary Integrity Mandatory Integrity Physical Integrity Rollback Separation of Duties Self Testing
3 **Availability**	Containment Robustness Recovery
4 **Accountability**	Audit Identification and Authentication Trusted Path Pseudonymity [additional to CTCPEC]

Table 3: **Facets of Security** and Security Services as discussed in SC27/WG3

The following are the working definitions of the three additional security services:

(1) *Unobservability* ensures an entity may use a resource or service without others, especially third parties, being able to observe that resource or service is being used.

(2) *Anonymity* ensures that an entity may use a resource or service without disclosing its identity.

(3) *Pseudonymity* ensures that an entity may use a resource or service without disclosing its identity, but can still be held accountable for that use.

In March 1993 it was decided to give up the hierarchical structuring by facets of security, as there was no consensus on the matching of facets and services. Additionally four services were proposed by the German national body: Non-repudiation (as defined in [ISO 7498-2 1989]), reliability of service, accuracy and unlinkability. The services derived from the CTCPEC were retitled to “Mature Security Services” while the others still are left as working definitions for additional or “new” services.

3.6 Is there a proper Structure for Security Functionality?

By now every structure of security functionality brought forward was criticised for being incomplete or unsystematic. Completing a structure by adding new services is no hard technical problem any more as there are user and usee friendly services and service definitions available now. The main reason for the bias of current criteria on system owner’s security in the past seems to be the reluctance of national security agencies to accept the reality of networked systems and the demand as well as the right of users and usees to be protected.

Getting a systematic and well organized structure of security functionality seems to be technically hard or even impossible for at least two reasons:

(1) There is no sharp distinction between the basic properties (or facets) of security, but often proposals seem to be criticised merely for political than technical reasons (cf. 3.5).

(2) A lot of functions as they are discussed today serve for more than one facet of security, e.g. access control serves for confidentiality as well as for integrity. There seems to be a direct proportion between the popularity of a function definition and the number of security facets it covers. Simply dividing access control into read control and write control could help the systematic, but is not (yet) popular.

Criteria writers, especially SC27/WG3 might have to decide, whether they want just a long list of services or accept a structure, even if its divisions are not completely orthogonal. A possible solution might have two steps:

(1) Setting up facets and services fitting to the facets and working out dependencies between the facets and the services and possibly between both.

(2) Collecting security mechanisms as they are popular today, and working out the m:n-relationships between mechanisms and services.

Table 4 contains a possible structuring according to step 1 incorporating ideas from the structures discussed before.

1 **Confidentiality**	Read Control Unobservability of (communication) events Unlinkability of (communication) events Object Reuse Covert Channel Handling
2 **Integrity**	Modify Control (for prevention of damage) Rollback (if damage occured)
3 **Availability**	Containment (for prevention of damage) Robustness (for smaller repairs) Recovery (after a system break down)
4 **Accountability**	Non-Repudiation (to find responsible entities) Pseudonymity (to get compensation in the case of damage)

Table 4: **Facets of Security** and Security Services

One might miss “Anonymity” in this list, but it can be seen as a special case of unlinkability, because it is the unlinkability of an identity and a current or past event.

A list of security mechanisms includes:

- Identification;
- Authentication;
- Audit;
- Untraceable Communication Mechanisms;
- Administration of Rights;
- Separation of Duties;
- Role Models;
- Encryption;
- Self Testing;
- Physical Protection.

4 CONCLUSIONS

Writing evaluation criteria for IT security seems to be a hard job for all experts, but harmonising different evaluation criteria and certification systems often follows different rationales. The aims are easy to define but hard to reach:

(1) Reach mutual recognition of evaluation results and avoid this idea being overruled by protectionism.

(2) Include new knowledge about security and do not block the further development in security research by freezing the current state of the art as final result forever or even for a period longer than e.g. 4 years.

Criteria for good criteria are:

(1) The description of security functionality has to be restructured to include multilateral security functionality or at least to be an open list containing all headings which are needed for multilaterally secure systems. This could be demonstrated by example functionality classes or protection profiles covering a wide range of functionalities.

(2) The definition of functionality classes by independent bodies has to be sponsored to promote the recognition of legal regulations and different security needs, e.g. the rights of citizens as customers and users in telecom networks.

(3) The problems and risks of computer aided software engineering (CASE) have to be considered in the field of assurance. Especially the risks of transitive Trojan Horses in CASE tools, e.g., editors and compilers should be treated.

(4) Only cryptographic mechanisms whose complete construction and design decisions are internationally known and discussed are eligible for high ratings.

(5) As long as only parts of security are understood, the title and the scope section of criteria have to be written in a modest way to avoid misunderstandings about their content and applicability.

To get high quality multilateral security evaluation criteria the development process must have high quality:

(1) The organisation of the criteria development and hormonization process has to be public and open and with a public rationale. Issues of usees who normally lack the ability to appear and speak for their interests, must be stressed, e.g. in the classical ISO standardisation process “usee representatives” must be sponsored to visit *and* prepare the meetings.

(2) Complete and detailed synopsises of the criticism and a rationale for the reaction of the authors have to be published.

(3) The criteria have to be tested by users who need open systems.

Further requirements relate to evaluation and certification schemes:

(1) The use of IT security certificates and certified products must not replace careful local risk analyses and security considerations at the places where the information is processed.

(2) Products and systems must be re-evaluated continuously even after a certification e.g., to cover new arising threats. Therefore the validity of a certificate might have to be limited.

(3) The evaluation and certification organisations have to be evaluated, too. If many organisations do evaluation and certification a common basis for the accreditation of these organisations is needed. The concept of *one* organisation having a monopoly on the certification of systems and products as well as on the accreditation of evaluation facilities has to be rethought.

(4) The public and international rating of cryptographic mechanisms has to be *organized* internationally.

The eastern European countries are in a special situation. They combine highly skilled experts with a lack of IT and a lack of telecommunication infrastruture. Also evaluation and certification schemes for IT security are not developed very well. Democratic structures are to be established in several areas. It might be easy just to copy current techniques and structures from western countries, and often the urgent need might propose this sort of solutions. At least two infrastructures should be considered and tested very well, e.g. by prototypical experiments, before final decisions and long-term commitments are made, as both may have a major influence on the – hopefully – democratic development of new countries

(1) The telecommunication infrastructure and the organisational questions around.

(2) Evaluation, certification and accreditation schemes for multilaterally secure IT systems.

This might help the new countries in eastern Europe to make good use of the mistakes made and the lessons learned in other countries.

5 ACKNOWLEDGEMENTS

Virgil Gligor sent helpful email on dependencies, Andreas Pfitzmann helped with faxes and intensive discussions on the phone, Ulrich Kohl entered helpful hints into early and late versions of this text, Herbert Damker helped getting the final print out of the printer.

6 REFERENCES

[Brunnstein, Fischer-Hübner 1990] Klaus Brunnstein, Simone Fischer-Hübner: Risk Analysis of “Trusted” Computer Systems; Proceedings of the 6th International IFIP TC-11 Security Conference on Information Security, Sec’90, May 1990

[Brunnstein, Fischer-Hübner 1992] Klaus Brunnstein, Simone Fischer-Hübner: Möglichkeiten und Grenzen von Kriterienkatalogen; Wirtschaftsinformatik, Vol. 34, No. 4, August 1992, p. 391-400

[Bürk, Pfitzmann 1990] Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) p. 715-721

[CEC 1990] (Informal) EC advisory group SOG-IS: Information Technology Security Evaluation Criteria (ITSEC), Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom – Version 1; 02 May 1990

[CEC 1991] (Informal) EC advisory group SOG-IS: Information Technology Security Evaluation Criteria (ITSEC) – Provisional Harmonised Criteria – Version 1.2; 28 June 1991, 163 pages, Office for Official Publications of the European Communities, ISBN 92-826-3004-8

[CESG 1989] UK Systems Security Confidence Levels, CESG Memorandum No.3, Communications-Electronics Security Group, United Kingdom, January 1989

[Chaum 1985] David Chaum, Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044

[CSSC 1992] Canadian System Security Centre: The Canadian Trusted Computer Product Evaluation Criteria, Draft Version 3.0e; 29 April 1992, 240 pages, Communications Security Establishment, Government of Canada

[CSSC 1993] Canadian System Security Centre: The Canadian Trusted Computer Product Evaluation Criteria, Version 3.0e; January 1993, 233 pages, Communications Security Establishment, Government of Canada

[DTI 1989_1] DTI Commercial Computer Security Centre Evaluation Manual, V22; DTI, UK, February 1989

[DTI 1989_2] DTI Commercial Computer Security Centre Functionality Manual, V21; DTI, UK, February 1989

[ECMA 1993] European Computer Manufacturers Association: Commercially oriented Functionality Class – Draft 6 – Working Paper; 09 February 1993, Gottfried Sedlak, ECMA Technical Committee 36

[Gehrke, Pfitzmann, Rannenberg 1992] Michael Gehrke, Andreas Pfitzmann, Kai Rannenberg: Information Technology Security Evaluation Criteria – a Contribution to Vulnerability? in: INFORMATION PROCESSING 92 – Proceedings of the IFIP 12th World Computer Congress Madrid, Spain, 7-11 Sept. 1992, ed. by R. Aiken, p. 579-587

[GI 1992] Privacy Protection and Data Security Task Force of the German Society for Informatics: Statement of Observations concerning the Information Technology Security Evaluation Criteria (ITSEC) V1.2; 24 February 1992, edited in Data Security Letter, No. 32, April 1992, original version available from the author

[GISA 1989] German Information Security Agency: IT-Security Criteria, Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems; January 1989, Bundesanzeiger-Verlag, ISBN 3-88784-200-6

[ISO 7498-2 1989] International Organisation for Standardisation: Information Processing Systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, International Standard ISO IS 7498-2, First edition 1989-02-15.

[JEIDA 1992] Japanese Electronic Industry Development Association: Computer Security Evaluation Criteria – Functionality Requirements, Draft V1.0; 31 August 1992, 30 pages, Special Committee for Security Evaluation Criteria, JEIDA, 3-5-7 Shiba-koen, Minato-ku, Tokyo 105, Japan

[Kaspersen 1992] Henrik Kaspersen: Security measures, standardisation and the law, in: INFORMATION PROCESSING 92 – Proceedings of the IFIP 12th World Computer Congress Madrid, Spain, 7-11 Sept. 1992, ed. by R. Aiken, p. 393-400

[Pfitzmann, Pfitzmann, Waidner 1991] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with very small Bandwidth Overhead; Proc. IFIP/Sec'91, Brighton, UK, May 1991; North-Holland; Amsterdam 1991; 245-258

[Rihaczek 1991] Karl Rihaczek: The Harmonised ITSEC Evaluation Criteria; Comp. & Sec. 10 (1991) 101-110

[SCSSI 1989] Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information, 692/SGDN/DISSI/SCSSI, Service Central de la Sécurité des Systèmes d'Information, Juillet 1989.

[US_DOD 1983, 1985] DoD Standard: Department of Defense Trusted Computer System Evaluation Criteria; December 1985, DOD 5200.28-STD, Supersedes CSC-STD-001-83, dtd 15 Aug 83, Library No. S225,711

[US_NCSC 1987] United States National Computer Security Center: Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria – Version 1; 31 July 1987, NCSC-TG-005, Library No. S228,526

[USA_NIST 1992] United States National Institute for Standards and Technology: Minimum Security Requirements for Multi-User Operating Systems – Issue 2; 07 August 1992, 54 pages, Computer Security Division, Computer Systems Laboratory, NIST

[US_NIST_NSA 1992] United States National Institute for Standards and Technology & National Security Agency: Federal Criteria for Information Technology Security – Draft Version 1.0; December 1992, 2 volumes