THE COMMON CRITERIA AND INFORMATION SYSTEMS SECURITY CERTIFICATION

Nikolaos C. Kokkinos
Kavala Institute of Technology (KIT), Faculty of Engineering
Department of Petroleum Technology
Ag. Loukas, 65404 Kavala, Greece
e-mail: nikokkinos@mwpc.gr

Dimitrios I. Maditinos
Kavala Institute of Technology (KIT), School of Business and Economics
Department of Business Administration
Ag. Loukas, 65404 Kavala, Greece
e-mail: dmadi@teikav.edu.gr

Željko Šević
Glasgow Caledonian University, Glasgow School for Business and Society,
Cowcaddens Road,Glasgow G4 0BA, UK
e-mail: Zeljko.Sevic@gcal.ac.uk

Aleksandar Stojanovic
University of Greenwich, Business School,
MG QA148, KW231, Greenwich, London, UK
e-mail: A.Stojanovic@greenwich.ac.uk

Abstract

Information security is a vital business requirement in today's information systems (IS). Last decades, the prospect of information technology security evaluation became a great worldwide challenge for many national institutes, agencies and schemes. Eventually, on the road to international harmonisation the Common Criteria Editorial Board (CCEB) managed to establish a common worldwide platform and called it: Common Criteria for Information Technology Security Evaluation (known as CC).

Purpose: The number of the information threats and violations are increasing while technology is developing. The need for certifying the efficiency and the safety of an IS is a fundamental business issue. This paper discusses the sufficiency of the CC IS security evaluation-certification and it is intended to shed light to the shortcomings of the CC.

Design/methodology/approach: The Common Evaluation Methodology (CEM, 2009) has been studied and used in order to examine the security certification of IS.

Findings: The results of the specific study revealed the weaknesses of the CC international standard to evaluate and to certify an IS as a secure one. No matter to what extent the components products of an IS have been evaluated, when they are combined and connected into a network or system, further security issues are going to arise. Moreover, the information system security evaluation takes time, but the Target Of Evaluation (TOE) belongs to a very frequently changing world. On the other hand, an IS comprises not only hardware, software and networks, but also people; and the prediction of human error and its frequency in a Protection Profile (PP) is very close to a practical impossibility.

Research implications: There is a fundamental requirement for better assurance of IS and for a continuous improvement of the common worldwide security evaluation platform, which is called Common Criteria.

Originality/value: This study opens a road to an essential and efficient information system security evaluation, which is a common concern for every business or enterprise.

Keywords: information systems security, information security management standards, information security certification.

1. INTRODUCTION

The concern for information security starts with the first appearance of computer networks. The essential pillars of information security continue to be until now the confidentiality (prevention of the unauthorised

disclosure of information), integrity (prevention of the unauthorised modification of information) and availability (prevention of the unauthorised withholding of information or resources). Information is a key aspect in the success of any e-business. As more information is created, stored and moved around computer networks, so the associated risk increases as well as the vulnerability of source data. Last decades the prospect of IT security evaluation became a great worldwide challenge for many national institutes, agencies and schemes (Cugini, 1995). Eventually, on the road to international harmonisation an International Standard ISO/IEC 15408 was developed based upon the Common Criteria for Information Technology Security Evaluation (CC). However, in spite of the fact that the current version of CC (2009) refers also to system evaluation, this study reveals that the CC are unable to evaluate, to certify and to accredit an information system (IS) as a secure in whole. Furthermore, various important drawbacks of CC need to be solved in order this international united attempt in the neuralgic field of security evaluation to continue existing and being improved.

2. THEORETICAL BACKGROUND

2.1 Historical review of IT security evaluation

The origin of the information systems security evaluation stems from the United States (US) in the end of 1960s. According to Ware (1970), in October 1967 the Advanced Research Projects Agency (ARPA) assigned a task force to thoroughly study and recommend appropriate computer security safeguards that would protect classified information in multi-access, resource-sharing computer systems. It is worthy of remark that those days the Arpanet, the parent of the Internet, was in its infancy and the revolution of the personal computers had not yet occurred. The confidential final report of the task force was published by The Rand Corporation (1970) for the Office of the Director of Defence Research and Engineering - the report was declassified by the Defence Advanced Research Projects Agency in 1975. Almost for one decade, the above mentioned report, known as Rand Report R-609, along with Anderson's (1972) later study were the most prominent comprehensive discussions for the information systems security.

In 1981, the National Computer Security Centre (NCSC) was established in US and after two years it published the first official security evaluation standard which was named Trusted Computer System Evaluation Criteria (TCSEC), known as Orange Book. Undoubtedly, the TCSEC was the precursor to the next developments of IT security evaluation criteria (ITSEC, 1991). According to the updated DoD TCSEC (1985), the purpose of the TCSEC was the evaluation and accreditation of the overall Automatic Data Processing (ADP) system security policy. The TCSEC consisted of four divisions: D, C, B and A. The division A (the highest security assessment) and the divisions C, B and A were divided into a series of hierarchical subdivisions called classes: C1, C2, B1, B2, B3 and A1. Since the first publication of the Orange Book and until the early 1990s, many other important Books were published by Rainbow Series of NCSC as updates of the TCSEC, like the publication of the Trusted Network Interpretation (TNI, 1987), known as the Red Book, which was nothing more than a network context of the Orange Book.

On the other hand in Europe (1990), the corresponding agencies from France, Germany, the Netherlands and the UK decided to cooperate in order to build and adopt a common IT security evaluation policy better fitted to the needs of the European Community. The new IT security evaluation policy would be based upon the existing IT security criteria of:

a) The US Department of Defense Orange Book (DoD TCSEC, 1985),
b) The UK Communication and Electronic Security Group Memorandum Number 3 (UK Systems Security Confidence Levels, 1989),
c) The proposals of the Department of Trade and Industry, known as the Green Book (DTI Commercial Computer Security …, 1989)
d) The German Information Security Agency (Criteria for the Evaluation of Trustworthiness ..., 1989)
e) The French Central Service of Information System Security, the so-called "Blue-White-Red Book" (Catalogue de Critères …, 1989)

The result of the above cited harmonised effort was the development of a security evaluation criteria set known as Information Technology Security Evaluation Criteria (ITSEC, 1991). The ITSEC became the foundation for the joint DTI/CESG Scheme, which was launched in 1992. According to Harris and Hunt (1999), the ITSEC places emphasis on integrity and availability, and attempts to provide a uniform approach

to the evaluation of both products and systems. Herson (2000) noted that both US and Japanese products began coming to Europe to be evaluated. The ITSEC defined seven assurance levels: E0, E1, E2, E3, E4, E5, and E6. The assurance level E0 was reserved for products that failed evaluation, while El to E6 represented increasing assurance. Moreover, a common methodology (known as ITSEM) defined both how evaluations should take place and how they should be certified. Roles of Developers in ITSEC (1996) provided a general indication of the appropriate time to have a product evaluated under the ITSEC scheme: For assurance level E1 up to 6 months, for E2 6 to 18 months, for E3 8 to 24 months and for E4 and higher the evaluation took several years.

The rest international community adopted various related approaches. In 1993, the Canadians developed the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), which were very similar to the TCSEC, but they had included also features of the ITSEC in order to enable its application to a wider range of products and systems (CTCPEC, 1993; Harris and Hunt, 1999). In Australia the Defence Signals Directorate (DSD) announced the establishment of the Australian Information Security Evaluation Programme in June 1994. Australia and New Zealand merged their evaluation and certification capabilities in 1998, and the AISEP was renamed to Australasian Information Security Evaluation Program. On the other hand, US made an effort to revise-replace the TCSEC with more flexible criteria and so, the National Institute of Standards and Technology (NIST) and the US National Security Agency developed the Federal Criteria (FC) for IT Security. Though a draft version was released for public comment in December 1992, however, this effort was overtaken by the Common Criteria and the FC never progressed beyond the draft stage (FC, 1992).

In June 1993, the European Commission, the US and Canada, took a decision to try to develop the Common Criteria for IT security evaluation. The authors of the TCSEC, ITSEC, CTCPEC and FC made a paramount combined effort to align-merge their criteria and create a single draft of the CC. Eventually the Common Criteria Editorial Board (CCEB) managed to establish a common worldwide platform and called it: Common Criteria for Information Technology Security Evaluation (CC). A draft version (ver. 0.9) was issued for public comment in October 1994 and the first version of CC (ver. 1.0) in January 1996. Then, on 7 November, 1996, in Brussels, Belgium, the European Commission hosted a full day conference on security evaluation and common criteria. Furthermore, representatives from US, Canada, UK, France, and Germany signed an agreement in Paris, on 12 March, 1998, for directly recognition of certificates issued by each other. On October 5, 1998, the above CC partners officially signed a Mutual Recognition Arrangement (MRA). The purpose of the MRA (then CCRA) is to formalize and promote a situation in which IT products that earn a CC certificate can be recognized by member nations without the need for re-evaluation and re-certification (Herson, 1996; Hickson, 1997). In 1999, the ISO/IEC approved the CC as an International Standard ISO/IEC 15408 and opened the way to the worldwide mutual recognition of evaluation results. ISO15408 security evaluations are performed by independent, accredited evaluation organisations, which are licensed by an appropriate certification body. The current version of CC is ver3.1R3 (CC, 2009).

2.2 Common criteria structure

The CC consist of requirements for the security evaluation, certification and accreditation of IT systems and products (TOE - Target Of Evaluation). These requirements are separated into the distinct categories of functional requirements (CC, 2009:Part 2) and assurance requirements (CC, 2009:Part 3). The CC functional requirements define desired security behaviour and the assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly (CC, 2009:Part 1). The CC discuss security using a hierarchical framework of security concepts and terminology. So, the CC are grouped into modular structures which are called components and they consist of indivisible statements of security needs named elements. The set of components that share a similar goal is called family and the groups of families that share a common intent are called classes. Moreover, the CC evaluation is based upon the concept of a Protection Profile (PP), which is nothing more than a platform of security specifications for a category of products, in order the security target (ST) to be achieved (Cugini, 1995). After all, the final CC Evaluation Assurance Levels range from EALl to EAL7, where EAL2 to EAL7 represented increasing assurance (and correspond very much to ITSEC El to E6).

3. COMMON EVALUATION METHODOLOGY

The well-known Common Evaluation Methodology (CEM, 2009) has been studied and used in order to examine the security certification of Information Systems. CEM (2009:13) quoted: "The Common Methodology for Information Technology Security Evaluation (CEM) is a companion document to the Common Criteria for Information Technology Security Evaluation (CC). The CEM defines the minimum actions to be performed by an evaluator in order to conduct a CC evaluation, using the criteria and evaluation evidence defined in the CC." Thus, the target audience for the CEM is primarily evaluators applying the CC and certifiers confirming evaluator actions. An evaluation is either both successful and granted a CC rating, or it simply does not get a rating. Unlike the ITSEC where a failed evaluation denotes as E0, CC has no concept of a failed evaluation such as EAL0 (Madsen, 1998).

4. RESULTS AND DISCUSSION

An information system comprises hardware, software, networks and people. According to CC (2009) and CEM (2009), the common criteria can specify-cover security issues for hardware, software and mainly, for the messages transferring over a network. In addition, an inherent shortcoming of IT evaluations is that the various TOE are examined independent of the real environment in which they use to operate. This means that, no matter to what extent the component products of an IS have been evaluated, when they are combined and connected into a network or system, further security issues are going to arise due to the complex interactions between the variety of products. Thus, the use of evaluated IT products in a network would not purge the system-level work, but it would reduce the probability of expensive errors (Mason, 2000). However, the most important component of an information system is people. The development of such a PP where the human resources would be evaluated and furthermore, the human error would be detected and not only the on purpose attacks is infeasible with CC standard. Subsequently, the total information system cannot be evaluated through the CC mechanisms.

Also, the current version of CC (2009) is a quite complex and large document of more than 1,000 pages, even for those who are familiar with standards. Moreover, the PPs created under CC are also complicated documents and by themselves could be International Standards, individually. It is worthy of remark that there is not automatic method of evaluation, which could facilitate the whole process of assessment. Therefore, the concept of developing user-friendly CC and/or PPs documentation and also, the automation of routine procedures would be an indeed progress as well as a wide spread of IS security evaluation.

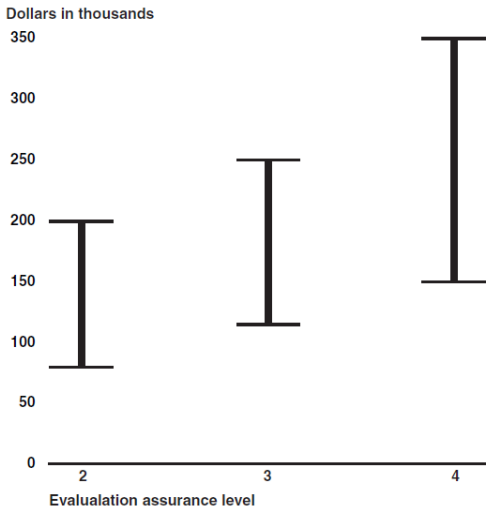

Figure 1. Range of sample cost of NIAP evaluations to vendors by EALs
Source: Information Assurance National Partnership ... (2006)

According to the Government Accountability Office (Information Assurance National Partnership ..., 2006), it was revealed that IT security evaluation takes noteworthy time and has a significant cost. For instance, for EAL4 a vendor has to spend $140,000 to $350,000 (Figure 1) and the whole evaluation process takes from 8 to 24 months (Figure 2). According to laboratory officials, the average time for vendors to

complete the required documentation before test and evaluation can begin is about six months (Information Assurance National Partnership ..., 2006). While the information system security evaluation takes time (e.g. many years for EAL5 to EAL7), the TOE belongs to a very frequently changing world and also, PP and ST maintain a slow updating rate. As a result, the evaluation delays getting the vendors' product to the market. On the other hand, the evaluation cost maybe is reasonable for large-scale IT companies, but for small or medium-scale IT companies which develop a unique product the unit cost per product is high. In both matters of time and cost, CCEB continues to appear a lack of solution even after thirteen (13) years from the recognition of CC as an International Standard ISO/IEC. Perhaps, this delay of response to the demands of the market by CCEB leads the vendors to an ignorance of CC or worst to a fatal ignorance of IT security. Table 1 illustrates a perturbing decreasing tendency in the CC certified products, since the positive peak of year 2007. In the same table, it is also notable that since 1998, only 1,785 products were certified and only 4 achieved the EAL7.

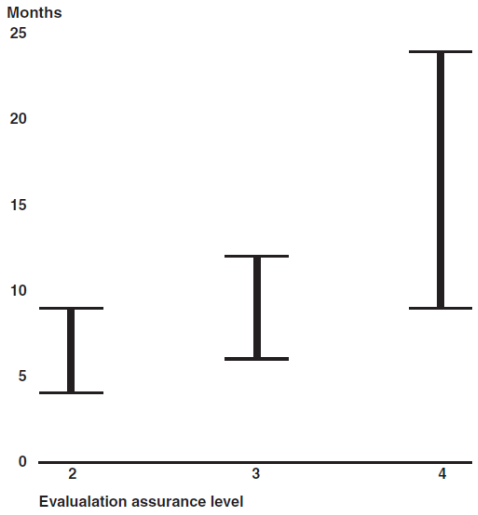

Figure 2. Range of time required for completing product evaluations at various EALs
Source: Information Assurance National Partnership ... (2006)

Table 1

Certified products by assurance level and year of certification

EAL \ Year	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	Total
EAL1	0	0	0	0	0	1	0	0	1	26	3	1	0	2	2	**36**
EAL1+	0	1	0	0	0	0	0	0	0	17	2	2	6	2	0	**30**
EAL2	0	0	0	2	2	1	6	13	16	113	29	17	6	12	0	**217**
EAL2+	0	0	0	0	1	1	1	1	2	57	21	29	21	38	19	**191**
EAL3	0	0	0	0	2	0	7	5	5	75	22	35	35	32	11	**229**
EAL3+	0	0	0	1	0	0	2	2	4	63	17	25	22	36	22	**194**
EAL4	1	0	2	2	3	1	0	1	0	72	6	11	6	6	1	**112**
EAL4+	0	0	1	1	3	3	2	8	4	207	75	90	67	77	35	**573**
EAL5	0	0	0	0	0	0	0	0	0	7	3	2	0	0	0	**12**
EAL5+	0	0	0	0	0	0	0	0	0	52	28	31	38	27	4	**180**
EAL6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**
EAL6+	0	0	0	0	0	0	0	0	0	0	1	2	3	1	0	**7**
EAL7	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	**2**
EAL7+	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	**2**
Basic	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Medium	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**

US Std	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**
None	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Totals:	**1**	**1**	**3**	**6**	**11**	**7**	**18**	**30**	**32**	**691**	**207**	**246**	**205**	**233**	**94**	**1785**

Source: Common Criteria (2012)

5. CONCLUSIONS

CC security evaluation was a unique, incredible worldwide achievement of paramount combined and united efforts from different countries. The history of CC was indeed brilliant. However, if the CCEB desires to have also a brilliant and successful future, the CC security evaluation needs to be changed - improved now more than ever before. This is in line with the keynote speaker Szakal (2011:19) in the 12th International Common Criteria Conference (ICCC) in Kuala Lumpur, who mentioned that: "Without a structural/group dynamic change, Common Criteria reform will stagnate and become less relevant. An unreformed and unreformable CC will degrade, fragment and… become increasingly irrelevant". The results of the current study revealed the weaknesses of the CC international standard to evaluate, to certify and to accredit an IS as a secure one. Moreover, the complexity of documentation, time-consuming procedures, lack of automatic routines and the significant cost of CC security evaluation remain unsolved for many years. Our research group works on that direction and aspires to develop integrated models that would be depended on the actual industrial environment of IS and they will contibute to the long-awaited solution of the security evaluation shortcomings.

REFERENCES

1. Anderson, J.P. (1972), *Computer Security Technology Planning Study,* ESD-TR-73-51, Bedford, MA: Hanscom AFB.
2. "Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)" (1993), *Communications Security Establishment*, January 1993, Ver. 3.0e.
3. "Catalogue de Critères Destinés à évaluer le Degré de Confiance des Systèmes d'Information" // "Catalog of criteria for evaluating the degree of confidentiality of Information Systems" (1989), *Service Central de la Sécurité des Systèmes d'Information*, July 1989, 692/SGDN/DISSI/SCSSI.
4. Common Criteria (2012), "Certified Products List-Statistics", available at: http://www.commoncriteriaportal.org/products/stats/ (accessed: 10 August 2012).
5. "Common Criteria for Information Technology Security Evaluation (CC)" (2009), *Common Criteria Recognition Arrangement Development Board*, July 2009, Part 1-3, Ver. 3.1R3.
6. "Common Methodology for Information Technology Security Evaluation (CEM)" (2009), *Common Criteria Recognition Arrangement Development Board*, July 2009, Part 1-3, Ver. 3.1R3.
7. "Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems" (1989), *German Information Security Agency*, January 1989, ISBN 3-88784-200-6.
8. Cugini, J. (1995), "The Common Criteria: On the Road to International Harmonization", *Computer Standards and Interfaces*, 17(4), 315-320.
9. "Department of Defense Trusted Computer System Evaluation Criteria (DoD TCSEC)" (1985), *Department of Defense*, 26 December l985, DoD 5200.28-STD.
10. "Description of the AISEP Australian Information Security Evaluation Programme" (1997), *Defence Signals Directorate*, March 1997, Memorandum No. 1.
11. "DTI Commercial Computer Security Centre Evaluation Levels Manual" (1989), *Department of Trade and Industry*, February 1989, V22.
12. "Federal Criteria for Information Technology Security (FC)" (1992), *National Institute of Standards and Technology / National Security Agency (NIST/NSA)*, December 1992, Ver. 1.
13. Harris, B. & Hunt, R. (1999), "Firewall certification", *Computers and Security*, 18(2), 165-177.
14. Herson, D. (1996), "European Conference on Security Evaluation and Common Criteria", *Computer Fraud and Security*, 1996(12), 6.
15. Herson, D. (2000), "The Changing Face of International Cryptography Policy: Part 8 - Common Criteria", *Computer Fraud and Security*, 2000(1), 8-9.
16. Hickson, N. (1997), "Security Evaluation and Certification: The Future of a National Scheme", *Information Security Technical Report*, 2(1), 6-28.

17. “Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria” (1991), *Commission of the European Communities*, June 1991, COM(90) 314, Ver. 1.2.
18. “Information Assurance National Partnership Offers Benefits, but Faces Considerable Challenges” (2006), *United States Government Accountability Office*, March 2006, GAO-06-392.
19. Madsen, W. (1998), “Racing for Common Criteria Certification”, *Computer Fraud and Security*, 1998(7), 8.
20. Mason, D.T. (2000), “Platform Security and Common Criteria”*, Information Security Technical Report*, 5(1), 14-25.
21. “Roles of Developers in ITSEC” (1996), *UK IT Security Evaluation and Certification Scheme*, July 1996, No. 4.
22. Szakal, A.R. (2007), "Strategy for Increasing Common Criteria's Global Influence and Recognition", in *12th International Common Criteria Conference (ICCC), 27-29 September, 2011*, Kuala Lumpur: ICCC, 19.
23. “Trusted Network Interpretation (TNI)” (1987), *National Computer Security Center*, 31 July 1987, NCSC-TG-005.
24. “UK Systems Security Confidence Levels” (1989), *Communications-Electronics Security Group*, January 1989, Memorandum No. 3.
25. Ware, W.H. (1970), *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security*, AD # A076617/0, Santa Monica, CA: The RAND Corporation.