Common Criteria: A Survey of Its Problems and Criticism

Technical Report[1]

Jim Yuill

2008

Abstract: The Common Criteria (CC) is a computer-security standard that some governments use for procurement, e.g., the U.S. Department of Defense. To sell information-security products in these markets, CC certification is required. Much has been published about problems with CC, and there is extensive criticism of CC. For example, a director of the U.S. CC program was recently quoted as saying, "Defending the program is a full-time effort. It is a difficult job." This paper presents a survey of the problems and criticism reported about CC. The paper provides: (a) a categorization for the reported problems, (b) a survey of the reported problems, organized by category, and (c) an annotated guide to the sources that were especially useful and authoritative. This paper is intended as a resource for those who are: evaluating CC for possible use, preparing to use CC, or researching CC itself.

1 Introduction

The Common Criteria (CC) is a computer-security standard that some governments use for procurement, e.g., the U.S. Department of Defense. To sell information-security products in these markets, CC certification is required. Much has been published about problems with CC, and there is extensive criticism of CC. For example, a director of the U.S. CC program was recently quoted as saying, "Defending the program is a full-time effort. It is a difficult job" [Jac07c]. In addition, the U.S. Government Accountability Office (GAO) has raised significant concerns about the U.S. CC program [Arn06, GAO06]. This paper presents a survey of the problems and criticism reported about CC.

This paper is based on a broad review of the CC literature from government, industry, and research. The focus was on literature critical of CC. The paper provides: (a) a categorization of the problems reported about CC, (b) a survey of the reported problems, organized by category, and (c) an annotated guide to the sources that were especially useful and authoritative. This paper is intended as a resource for those who are: evaluating CC for possible use, preparing to use CC, or researching CC itself.

In reporting problems about CC, we are primarily repeating what others have said, and only a few of the reported problems are our own observations. Also, for most of the problems reported, multiple sources are cited. (A total of forty-nine sources are cited.) The following sections present, respectively: an overview of CC, a survey of CC problems and criticism, and an annotated guide to useful sources. A subsequent section explores problems that stem from the CC program being a government program and operated under government management. A final section concludes.

[1] This technical report is part of a research project at North Carolina State University in 2008. The report was presented at a computer-security conference, in slide format: "Common Criteria: A Survey of its Problems and Criticisms," DoD Cyber Crime Conference 2009, St. Louis, MO, January 2009.

2 Overview of CC

CC is a government program for certifying the security functions of computer products, e.g., firewalls [CC08a]. CC is developed by a consortium of government agencies from a number of countries [CC08a]. The U.S.'s CC program is called The Common Criteria Evaluation and Validation Scheme (CCEVS) [CCE08]. CCEVS is run by NIST and NSA, but mostly by NSA [Jac07a].

It appears that, in practice, CC is only used in government procurement [Bid07, CCU04, Hea04, Jac07a, Pta06, Rag07]. CC provides security standards that vendors must meet in order to sell computer products to governments, e.g., to sell firewalls to the U.S. Department of Defense (DoD) [CCE08, GAO06, Mal05, Sch03, Wai06]. In the U.S. Federal Government (USFG), CC certification is only required for information-security products used in national-security systems [GAO06]. These are systems that contain classified information or involve intelligence activities.

CC provides a process for governments to specify security requirements for types of computer products that they purchase, e.g., security requirements for firewalls [CC08b, CC08c]. These computer products can include hardware, software, and firmware. CC applies to devices and not to IT systems. For a particular product type, the security requirements are specified in a *Protection Profile* (PP). For example, PPs have been developed for various types of firewalls. One such PP is named "Firewall with limited requirements." The CC website lists all of the Protection Profiles [CC08a].

CC also has a process for a vendor to demonstrate that its product complies with a PP's security requirements [CC08d]. The requirements for demonstrating compliance are specified by an *Evaluation Assurance Level (EAL)*. There are seven EALs, numbered from 1 to 7. In general, each EAL requires certain processes for product documentation, development, and testing. The higher numbered EALs involve more rigorous processes.

Each PP includes a specification of the EAL it requires. For example, in the PP "Firewall with limited requirements," EAL 4 is required [CC08a]. EAL 4 is summarized as requiring the product be "methodically designed, tested and reviewed" [CC08d].

To demonstrate that a product complies with a PP, CC provides an evaluation and certification process [CC08e]. For example, a firewall vendor could hire an approved third-party evaluator to certify that its product complies with the PP "Firewall with limited requirements".

In the CC documentation, CC is presented as a general-purpose process for providing security assurance, which could be used by any organization, private or public. CC is not presented as a means of assurance for government procurement. Also, the CC authors present the CC process in a way that is more general and abstract than the way we have described it here [CC08b, Syn]. CC provides a broad framework for vendors to make almost any type of security claim about almost any type of computer product. However, in practice, CC appears to only be used for government procurement.

In our judgement, the attempt to make CC be a general-purpose security-assurance process is a fundamental flaw in CC. First, a single general-purpose assurance-process does not seem possible, as assurance needs and requirements vary widely among systems and stakeholders. Second, portraying CC as a general-purpose assurance-process is a misrepresentation. In practice, CC is made for use as a government-mandated standard, for government procurement. And, that environment has assurance requirements that are unique to government management.

For example, government-mandated assurance standards must be highly objective, in order for the standards to be followed and enforced. Highly objective standards are also needed to guard against abuse, such as corruption and tyranny.

In contrast, private businesses have much greater liberty in using subjective judgement in procurement. (This is one reason why private businesses can operate more effectively than government [Mis44].) By nature, computer-security development involves a large degree of subjective judgement and wisdom, e.g., how much security is enough? And, computer-security assurance also involves a large degree of subjectivity, e.g., has the claimed security been provided adequately?

3 Survey of CC problems and criticism

The following sections summarize the problems reported about CC, from our literature survey. These sections also serve to categorize the reported CC problems. The top-level sections are: "Problems with CC's effectiveness," "Problems with CC's stated limitations," and "Problems with CC implementation."

3.1 Problems with CC's effectiveness

The primary complaints about CC have to do with its effectiveness. This includes concerns about CC's ability to improve security and provide assurance, and also concerns about CC's implementation costs.

- **CC does not substantially improve security:**

Many security professionals and company representatives assert that the CC process does not substantially improve security, nor is it cost-effective. This includes security professionals in industry [CCU04, Hea04, Jac07a, Jac07c, Pot06, Pta06, Wai06] and research [Sha03, SDN04, Sto05]. There are better ways to improve security [Bid07, CCU04, Pta06, SDN04, Sto05]. Also, it is not clear if CC is an effective means for improving government security [CCU04, Jon06a, Jon06b, Lau06, Spa03, Wai06]. The GAO analyzed the U.S. CC program. One of its primary criticisms was a lack of evidence regarding CC's performance and effectiveness [Arn06, GAO06]. A widely held view is that CC is not effective for use in non-government markets (i.e., commercial markets) [Bid07, CCU04]. Within the USFG, CC certification is only required for national-security systems. The GAO recommended against expanding CC use to systems not used for national-security [GAO06].

- **CC provides inadequate security assurance:**

A major concern about the CC process is that it is weak in detecting implementation bugs and vulnerabilities, and thus provides little assurance that a product is secure from attack [Bid07, Jac07a, Jac07c, Lau06, Pta06, Wai06]. A Symantec spokesperson states that, "Any software product can contain vulnerabilities, and there is nothing in the [CC] protection profile that provides any confidence or assurance to the customer that we've done a good job in that area ..." [Jac07c]. A member of the Microsoft security team states that, "Currently, Common Criteria fails to meet customer needs as a useful indicator of the likelihood of security vulnerabilities in software" [Bid07]. He goes on to say, "If CC simply validates conformance to a set of

documented security feature requirements, then CC needs to better communicate this limited scope to its customers in order to set expectations that it will 'help keep honest people honest' – but [it] is incomplete or inadequate in terms of assurance of the security of assets on a system."

A researcher at Johns Hopkins University raises similar concerns about CC's ability to provide assurance [Sto05]. He asserts that CC's concept of assurance differs from the security community's. Also, he argues that the CC evaluation-process is inconsistent with the way assurance is typically achieved in the marketplace, and that CC is not a cost-effective means for supplying assurance.

Thomas Ptacek describes how vendors have used their CC certification in misleading ways [Pta06]. These misleading advertisements take advantage of differences between CC's concept of assurance and consumers' expectation of a government assurance program. The actual meaning and significance of CC certification is carefully qualified on the CCEVES website [CCE08]:

> Certificates are not endorsements of the "goodness" of an IT product by NIST, NSA, or any other organization that recognizes or gives effect to the certificate. A certificate represents the successful completion of a validation that product met CC requirements for which it was evaluated/tested.

Although CC certification is not a government endorsement, vendors have used their products' CC certifications to imply government endorsement of their products. Ptacek provides several examples [Pta06].

- **Certification is lengthy and expensive:**

From our survey, one of the most frequent complaints about CC is that the certification process takes too long, and it is too expensive. These concerns are expressed by people in industry [Arn06, Bid07, Eri06, Jac07a, Jac07c, Lau06], research [RJM06, Spa03], and in government [GAO06, KS06, Rob03]. A Cisco representative stated that, ideally, the certification and accreditation process should take no more than six months, but 10 to 18 months is common [Arn06]. A systems engineer at Sun reports that certification takes about a year and a half. A member of the Microsoft security team reports that, "It typically takes 12 to 24 months or longer to complete an evaluation at the highest assurance levels (EAL4) that can be attained by general purpose commercial software products" [Bid07]. For a CC certification of Linux, compliance with EAL2 took four months, compliance with EAL3 took an additional six months, and compliance with EAL4 was estimated to be an additional 12 months [SK04]. A CC consultant reports that certification "is a medium-sized project. You will need someone to manage it, it will take several months of work, and will probably cost in the mid-six figures [(in U.S. dollars)]" [Rag07]. Another source reports that evaluation can cost from hundreds-of-thousands to millions of dollars [Jac06].

When government procurement requires CC certification, the lengthy CC certification process prevents acquisition of current technology [Arn06]. A member of the Microsoft security team reports that "CC evaluation results typically lag about one version behind the currently available version of a given product" [Bid07]. For vendors, the delays create risks for their products, including risks of obsolescence and risks of lost market opportunities [Arn06]. The high costs of CC certification can cause vendors to use their finite security budgets in non-optimal or ineffective ways [Pta06]. Also, the high costs of certification can exclude smaller vendors from government markets [Arn06, Pta06].

3.2 Problems with CC's stated limitations

The CC standards specify its limitations [CC08b].[2] Several of these limitations are areas of criticism.

- **Re-certification requirements are excessive:**

Once a product is evaluated and put in operation, previously unknown errors and vulnerabilities will inevitably surface. When the product is corrected, the evaluation results will not apply to the corrected version of the product [CC08b]. A CC consultant explains that re-evaluation requires going through the whole certification process again, though it may be easier and less expensive because vendors can re-use much of the evidence from the previous evaluation [Rag07]. He also notes that some countries have a simpler re-evaluation process, but it is only recognized within that country.

Both a vendor and a government-procurement official have reported that the mandated CC change-process is costly and time-consuming [Eri06, Wai06]. Professor Eugene Spafford raised concern about using CC for certifying systems that have extensive patching and customization needs [Spa03]. NIST and NSA spokespeople have recognized the need for CC to allow for re-evaluating product-changes and not the entire product [Jac07a, Rob03]. (This is the re-evaluation policy for the German CC process [BSI05].)

Another difficulty with CC is evaluating a product that has a single hardware base, but several versions of software that run on it. Apparently, CC would require evaluating the hardware for each version of the software. Some CC organizations have proposed a "composite evaluation" in which the hardware base is only evaluated once. Researchers have analyzed this scheme and reported problems with it [KK06].

- **Certification is only for a specific configuration:**

The CC process only certifies a system for a specific configuration, but in practice, it is likely that the system will be used in different configurations [Bid07, Jon06a, Jon06b, Lau06, Pot06]. This raises concerns about the usefulness of CC certification, as it does not provide explicit security assurance for these other configurations.

- **The operational environment is not evaluated:**

Another limitation is that the CC process does not evaluate the operational environment, and it assumes there is a "100% correct instantiation" of it [CC08b]. We did not find a clear definition of the operational environment.[3] Some examples that are given include the computer room of a bank, and a general office environment. Also, CC states it is only suitable for assessing the correctness of IT-countermeasures. However, non-IT countermeasures are also in the operational environment, and they are not evaluated (e.g., human security guards and procedures). For the operational environment, CC provides limited analysis and examination, and this is cited as a weakness [Hea04, Spa03].

---

[2] CC's introductory document describes CC's limitations [CC08b]. The sections that discuss limitations include: Chapter 2 "Scope", Section 7.1.3 "Correctness of the Operational Environment", Section 9.5 "Use of ST/TOE evaluation results", and Section A.6.4 "Assumptions".

[3] For example, in the CC introduction, its glossary defines the *operational environment* as: "the environment in which the TOE is operated" [CC08b]. (*TOE* is the Target of Evaluation.) This is a circular definition.

3.3 Problems with CC implementation

Another set of CC problems have to do with how it is carried out.

- **Incompatibilities with product lifecycles:**

There are incompatibilities between the CC process and industry's product lifecycles [Jac07a, KS06, Spa03, Wai06]. For example, CC is based on a development model that unrealistically expects system requirements to be known up-front. This concern is raised by those working with CC at the FAA and at Symantec [Jac07a, KS06]. Also, academic researchers have investigated CC's requirements process, and they have proposed improvements [MFP06, RZR07].

Concerns have been raised about CC's use with open-source software [Spa03, Whe06]. IBM sponsored a CC certification of Linux. A project retrospect has been published, and it includes discussion of the challenges encountered [SK04].

- **Vulnerabilities to vendor manipulation and to government misuse:**

The CC process is vulnerable to being manipulated by vendors seeking certification at minimal cost. Potential problems include shopping for the easiest certification requirements among CC member-states and among CC evaluators [AM07, Jon06a, SDN04]. Jeff Jones describes potential problems from certifying a minimal set of services [Jon06a, Jon06b].

The CC process is also vulnerable to being misused in government procurement. Problems have been reported about government buyers using CC certification requirements in ways that appear unjust for some vendors and that result in higher purchase prices [Wai06]. Also, a security expert at the SANS Institute holds that CC "has a lot of support in the international community, because labs in other countries can bring in hard currency from U.S. firms trying to get certified" [Wai06].

- **Large amounts of documentation:**

CC has the reputation of being a "paperwork exercise" [Jac06, Jac07c, Wai06]. This seems to be a statement about CC's effectiveness, and perhaps also, its volume of paperwork. Researchers at Johns Hopkins University report that, "The Common Criteria process is exceedingly difficult, not because it is conceptually hard to do but because it imposes an overwhelming burden of paperwork" [SDN04]. A certification project for Linux generated more than 800 pages of design, test, and evaluation documentation [SK04]. For certification projects, it is recommended to have a dedicated technical writer [CCU04].

- **Problems with CC's abstractions:**

In our own study of the CC documentation, we found CC was often framed so abstractly that it was difficult to understand. Typically, the difficulty was a lack of examples for making sense of the abstractions. For instance, one of CC's introductory documents states,

> A protection profile defines an implementation-independent set of security requirements and objectives for a category of products or systems which meet similar consumer needs for IT security. [Syn]

This statement would be much easier to understand if one knew that firewalls were one such category. Generally, abstractions are not meaningful without concrete examples as a reference.

Other researchers have reported problems from CC being too abstract, and making evaluation difficult [RJM06, VWW02].

- **Problems in using CC for IT systems:**

Some work has been done to adopt CC for use with IT systems (not just devices). However, significant problems were reported with its use at the U.S. Federal Aviation Administration (FAA) [KS06], and others have recommended against such use of CC [CCU04]. A member of the Microsoft security team holds that CC is effective in some bounded scenarios such as smart cards, but it is much less effective in scenarios with software that is of a larger scale and greater complexity [Bid07].

4 Useful sources

This section describes sources we found to be especially insightful and authoritative in our research of CC's problems and criticism.

4.1 Learning about CC

In learning about CC, we found the official CC documents to be the most useful, though the abstraction problems described earlier were significant [CC08b, CC08c, CC08d]. The CC organization commissioned a CC tutorial [Syn]. It was useful, but we also found it to be very abstract. We recently discovered a promising book on CC, by a CC consultant [Rag07]. It appears to be readable and useful, and it is freely distributed on the Internet. Two other books on CC have been published, though we have not read them [Her02, MB04].

To get concrete examples of CC use, we found a case study to be helpful [KL04]. In it, academic researchers used the CC process for a VPN. There are also published case studies from industry [Eri06] and for an open-source system (Linux) [SK04]. The ACM and IEEE databases are good sources for papers that present CC case studies (e.g., [PPH06]).

4.2 Government criticism

CC is a government program, so criticism of CC from within the government is especially revealing. The GAO analyzed the U.S. CC program and reported a set of problems with it [GAO06]. They report that these problems collectively hinder the effective use of the CC process by vendors and government agencies. The primary problems include: (a) difficulty in matching agencies' needs with the available evaluated products, (b) vendors' lack of awareness regarding the evaluation process, (c) a reduction in the number of validators to certify products, (d) a lack of performance measures for CC, and (e) difficulty in documenting the effectiveness of the CC process.

A manager of the U.S. CC program provided testimony on CC, and it includes a section on needed improvements [Rob03]. Criticism of CC, from within the government, is also quoted in trade magazines [Jac07c, Wai06] and in a report of the CC User's Forum [CCU04].

4.3 Industry criticism

Some of the most useful information about CC's problems is from vendors and security professionals that have implemented CC. They speak from first-hand experience, and they have borne the responsibilities, burdens, and risks of implementing CC.

The Common Criteria Users' Forum (CCUF) is one of the most useful sources of information we found. There, vendors reported problems in implementing Common Criteria. The vendors included Cisco, IBM, Microsoft, ORACLE, and Symantec. The first CCUF was held in 2004, and a summary report is available [CCU04]. A second CCUF was held in 2005 [CSI05], but based on our Internet searches, it appears that a summary report was not published. Also, it appears that additional CCUF's have not been held. One criticism of CC is that "industry input ... has little impact on the CC process as a whole" [Jac07c].

Some of the strongest criticism of CC comes from computer trade magazines [Arn06, Jac06, Jac07a, Jac07c, Pot06, Wai06]. These articles are recent, and they quote critics from industry, government, and research. A very critical article [Jac07c] prompted rebuttals from two CC apologists [Jac07b, Rat07].

Two papers in *IEEE Security & Privacy* are very critical of CC, and the writers have industry experience [Hea04, KS06]. One of these papers focuses on a CC extension that is intended for IT systems [KS06]. This excellent paper reports problems encountered in using this CC extension at the FAA [KS06]. Much of their analysis seems applicable to CC in general. Some of the problems they discuss are: (a) the use of inflexible standards in a system engineering-process that must be flexible, (b) the use of inflexible requirements (i.e., PPs) for systems that are deployed in diverse settings with diverse requirements, and (c) the imposition of standards that exceed developers' capabilities.

There are a number of insightful blog articles on CC, written by people experienced with CC. Two bloggers from Microsoft [Bid07, Jon06a, Jon06b] are critical of CC. An article by a computer-security consultant [Pta06] is also critical of CC. The article is accompanied by a lengthy forum discussion that is also very critical. Two bloggers—one from Sun [Lau06] and the other from IBM [Rat07]—are more supportive of CC, but they also discuss CC's limitations and weaknesses.

4.4 Researchers' criticism

Several university researchers have been extremely critical of CC. Dr. Spafford presented testimony on CC before the House Government Reform Committee [Spa03]. He presented a long list of problems with CC, and it is very insightful. Some researchers at Johns Hopkins University have also been very critical of CC [Sha03, SDN04, Sto05]. In one paper, Dr. Shapiro analyzes the CC certification obtained for Windows 2000 [Sha03]. He discusses weaknesses in the CC process, and he challenges CC's substance and credibility. The Slashdot website has an extensive discussion of this paper [Sla02]. In another paper, Dr. Stoneburner contends that CC's concept of assurance is contrary to the security community's, and that it is overly reliant on inspection [Sto05].

5 Problems from government management

Fundamentally, CC is a government program. CC is developed through government funding, and CC is used by vendors due to government mandates. In our judgement, CC's problems stem largely from government management and its inherent limitations and problems.

In government management, regulations must be highly objective, to ensure compliance and to guard against abuse [Mis44]. An earlier section described how computer-security development and assurance are inherently subjective, in some ways. A consequence is that government

mandates for computer-security assurance will have inherent limitations and problems. The limitations of government management in computer-security are further discussed in our report on security-engineering practices [Yui08].

Common Criteria's existence is the result of government fiat. CC's research and development is government funded. In 2004, it was reported that "governments from around the world have invested millions of dollars in the development of the [CC]" [CCUF04]. It appears that CC is only used in government sectors where its use is mandated. CC is not used appreciably, if at all, in the commercial sector. There are government sectors where CC use is not mandated. Although we have not found information about CC use in those government sectors, the GAO has recommended against CC being used there [GAO06].

The GAO reports that the CC program has not provided evidence of CC's effectiveness. Further, as reported here, a large number of credible sources assert that the CC program is not effective. This raises questions about why government CC programs continue, and why they continue to mandate the use of CC.

In his book *The Vision of the Anointed*, Thomas Sowell describes how government programs can become self-perpetuating bureaucracies [Sow96]. He provides examples of government programs that have persisted for decades with poor performance, and even after they increased the problems they were chartered to solve, e.g., poverty and crime.

One of the ways government programs become self-perpetuating is that they use their funding for self-promotion. This can occur in government-funded computer-science programs, in general. For example, in these programs, a primary measure of success is published papers and conference presentations. However, it is possible for such accomplishments to be more the result of government funding than useful research. Also, the people who develop and promote these programs typically have far more resources than those who investigate the programs' shortcomings and problems. These programs can also create strong biases in the programs' developers and practitioners, as their careers and finances depend upon the programs' continuance.

CC is a government-funded program whose use is mandated in government procurement. So, there is a need to guard against the CC program becoming an ineffective and self-perpetuating bureaucracy. Further, given the problems reported about CC from government, industry and research, there is reason to question if the CC program is such a bureaucracy.

6 Conclusion

CC has received a large amount of criticism from within government, industry, and research. This paper provides: (a) a categorization of the problems reported about CC, (b) a survey of the problems reported, organized by these categories, and (c) an annotated guide to sources about CC. In addition, we explored ways in which many of CC's problems appear to stem from government management, and its inherent limitations and problems.

In categorizing the problems reported about CC, the top-level categories are: (a) problems with CC's effectiveness, (b) problems with CC's stated limitations, and (c) problems with CC implementation. Overall, there are a substantial number of credible claims that CC is not effective at providing security assurance. And, the CC organization has not provided the cost-benefit analysis needed to assess CC's effectiveness.

This paper has focused on CC's problems, so it does not provide a complete picture of CC. Complete analysis of CC would include CC's benefits, as well as its problems. Further, in fairness, a complete analysis would include the CC organization's perspective of the problems reported about CC. We hope the CC organization will provide that.

Fundamentally, the CC organization's mission is to provide assessment and assurance. So, it is incumbent upon the CC organization to provide assessment and assurance about CC itself, including CC's problems and effectiveness. However, given the self-perpetuating nature of government programs, it would be very difficult for the CC organization to provide an objective assessment of itself, and especially if the findings would lead to a reduction in the organization's budget and power.

7 Bibliography

[AM07] Anderson, R. and T. Moore, "The Economics of Information Security: A Survey and Open Questions," *Proc. of the Fourth bi-annual Conference on the Economics of the Software and Internet Industries*, Toulouse, France, January 2007, Accessed May 25, 2008, http://www.idei.fr/activity.php?a=5875&lang=en.

[Arn06] Arnone, M., "GAO: Common Criteria is not common enough," *Federal Computer Week*, April 3, 2006, http://www.fcw.com/print/12_11/news/92813-1.html.

[Bid07] Bidstrup, E., "Common Criteria and answering the question 'Is it Safe'," Microsoft Security Development Lifecycle [blog], December 20, 2007, Accessed May 22, 2008, http://blogs.msdn.com/sdl/archive/2007/12/20/common-criteria-and-answering-the-question-is-it-safe.aspx.

[BSI05] Federal Office for Information Security (BSI), "BSI Certification and BSI Product Confirmation: Notes for manufacturers and vendors," BSI website, February 22, 2005, Accessed May 25, 2008, http://www.bsi.bund.de/zertifiz/zert/7138_e.pdf.

[CC08a] Common Criteria's website, Accessed May 1, 2008, http://www.commoncriteriaportal.org.

[CC08b] Common Criteria, "Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model," Version 3.1, Revision 1, Common Criteria's website, September 2006, Accessed December 2007, http://www.commoncriteriaportal.org.

[CC08c] Common Criteria, "Common Criteria for Information Technology Security Evaluation Part 2: Security functional components," Version 3.1, Revision 2, Common Criteria's website, September 2007, Accessed December 2007, http://www.commoncriteriaportal.org.

[CC08d] Common Criteria, "Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components," Version 3.1, Revision 2, Common Criteria's website, September 2007, Accessed December 2007, http://www.commoncriteriaportal.org.

[CC08e] Common Criteria, "Common Methodology for Information Technology Security Evaluation," Version 3.1, Common Criteria's website, September 2007, Accessed December 2007, http://www.commoncriteriaportal.org.

[CCE08] Common Criteria Evaluation and Validation Scheme (CCEVS), Accessed May 1, 2008, http://www.niap-ccevs.org/cc-scheme.

[CCU04] Common Criteria Users' Forum, "Common Criteria Users' Forum : Summary Report," Cyber Security Industry Alliance website, October 2004, Accessed May 1, 2008, http://www.csialliance.org/news/events/CCUF_Report_Final.pdf.

[CSI05] Cyber Security Industry Alliance (CSIA), "Recap of the Second Common Criteria Users' Forum (CCUF II)," *Cyber Security Industry Alliance Newsletter*, 1(11), CSIA website, July/August 2005, Accessed Mar 9, 2008, http://www.csialliance.org/news/newsletters/july2005/july_ccuf.html.

[Eri06] Eriksson, M, "How to develop secure IT products using Common Criteria," *Proceedings of the 2006 IEEE International Engineering Management Conference*, pp:297–299, September 2006.

[GAO06] Government Accountability Office (GAO), "Information Assurance : National Partnership Offers Benefits, but Faces Considerable Challenges," report GAO-06-392, GAO website, March 2006, Accessed May 16, 2008, http://www.gao.gov/cgi-bin/getrpt?GAO-06-392.

[Hea04] Hearn, J. "Does the common criteria paradigm have a future?", *IEEE Security & Privacy Magazine*, 2(1):64–65, Jan.-Feb. 2004.

[Her02] Herrmann, D. *Using the Common Criteria for IT Security Evaluation*, Auerbach, 2002.

[Jac06] Jackson, W. "Software insecurity: Plenty of blame to go around," *Government Computer News*, April 18, 2006. http://www.gcn.com/online/vol1_no1/40437-1.html.

[Jac07a] Jackson, J. "Symantec: Common Criteria is bad for you," *Government Computer News*, May 4, 2007, http://www.gcn.com/online/vol1_no1/44205-1.html.

[Jac07b] Jackson, W. "Mary Ann Davidson : In defense of common criteria," *Government Computer News*, October 8, 2007, http://www.gcn.com/print/26_26/45166-1.html.

[Jac07c] Jackson, W. "Under attack: Common Criteria has loads of critics, but is it getting a bum rap?," *Government Computer News*, August 13, 2007, http://www.gcn.com/print/26_21/44857-1.html.

[Jon06a] Jones, J. "The Importance of the 'Evaluated Configuration' in Common Criteria Evaluations," Jeff Jones Security Blog, May 24, 2006, Accessed May 1, 2008, http://blogs.technet.com/security/articles/430098.aspx.

[Jon06b] Jones, J. "JeffOS EAL4+ Secure System," Jeff Jones Security Blog, May 24, 2006, Accessed May 1, 2008, http://blogs.technet.com/security/archive/2006/05/24/430108.aspx.

[KK04] Karger, P. and H. Kurth. "Increased information flow needs for high-assurance composite evaluations," *Proceedings of the Second IEEE International Information Assurance Workshop*, pp:129–140, Charlotte, NC, April 2004.

[KL04] Kim, S. and C. Leem, "A Case Study in Applying Common Criteria to Development Process of Virtual Private Network," *Proceedings of the International Conference on Computational Science and Its Applications – ICCSA 2004*, Berlin/Heidelberg:Springer, May 2004.

[KS06] Keblawi, F. and D. Sullivan, "Applying the Common Criteria in Systems Engineering," *IEEE Security & Privacy*, 4(2):50-55, March/April 2006.

[Lau06] Laurent, J, "Solaris 10 has achieved Common Criteria evaluation!", Jim Laurent's Weblog, Accessed Dec 18, 2006, http://blogs.sun.com/jimlaurent/entry/faq_what_is_a_common.

[Mal05] Malnick, K, "Common Criteria: a prime factor in information security for the DoD," *Defense AT&L Magazine*, pp:30-33, January-February 2005.

[MB04] Merkow, M. and J. Breithaupt, *Computer Security Assurance Using the Common Criteria*, Thomson Delmar Learning, 2004.

[MFP06] Mellado, D., E. Fernandez-Medina, and M. Piattini, "A comparison of the Common Criteria with proposals of information systems security requirements," *Proceedings of the First International Conference on Availability, Reliability and Security (ARES 2006)*, April 2006.

[Mis44] Von Mises, L., *Bureaucracy*, Yale University Press, 1944.

[Pot06] Potter, R., "Perspectives: No Guarantee," *Information Security Magazine*, March 2006.

[PPH06] Pedersen, A., N. Partner, A. Hedegaard, and R. Sharp, "Designing a secure point-of-sale system," *Proceedings of the Fourth IEEE International Workshop on Information Assurance*, Royal Holloway, UK, April 2006.

[Pta06] Ptacek, T., "What Common Criteria Certification Means," also includes posted comments, Matasano Chargen's blog, June 19, 2006, Accessed May 1, 2008, http://www.matasano.com/log/331/what-common-criteria-certification-means/.

[Rag07] Ragen, A., *Manager's Guide To The Common Criteria*, Version 1.12, Alex Regan's home page, January 2007, Accessed May 21, 2008, http://www.alexragen.com.

[Rat07] Ratliff, E., "Widespread ignorance about Common Criteria," Emily Ratliff's blog, August 29th, 2007, Accessed May 25, 2008, http://www.ratliff.net/blog/index.php/2007/08/29/widespread-ignorance-about-common-criteria.

[RJM06] Razzazi, M., M. Jafari, S. Moradi, H. Sharifipanah, M. Damanafshan, et. al., "Common Criteria Security Evaluation: A Time and Cost Effective Approach," *Proceedings of the 2nd International Conference on Information & Communication Technologies – ICTTA '06*, 2:3287-3292, April 2006.

[Rob03] Roback, E., "Exploring Common Criteria: Can it Ensure that the Federal Government Gets Needed Security in Software?", Statement before the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, NIST website, September 17, 2003, Accessed May 1, 2008, http://www.nist.gov/testimony/2003/erobackcc.htm.

[RZR07] Romero-Mariona, J., H. Ziv, and D. Richardson., "CCARCH: Architecting Common Criteria Security Requirements," *Proceedings of the Third International Symposium on Information Assurance and Security, 2007 (IAS 2007)*, pp:349-356, August 2007.

[Sch03] Schaffer, J., "National Information Assurance Program -- Common Criteria Evaluation and Validation Scheme," *2003 Conference Proceedings: Egov OpenSource and SecurE-biz Executive Summit*, Crystal City, VA, April 2003, Accessed at Coolheads Consulting website May 1, 2008, http://www.coolheads.com/egov/securebiz/topicmap/s561/img19.html.

[SDN04] Shapiro, J., M. Doerrie, E. Northup, S. Sridhar, and M. Miller. "Towards a Verified, General-Purpose Operating System Kernel," *Proc. NICTA Invitational Workshop on Operating System Verification*, pp:1-19, Sydney, Australia, October 2004, Accessed at the Coyotos website May 23, 2008, http://www.coyotos.org/docs/osverify-2004/osverify-2004.html.

[Sha03] Shapiro, J., "Understanding the Windows EAL4 evaluation," *Computer*, 36(2):103-105, February 2003.

[SK04] Shankar, K. and H. Kurth, "Certifying open source - the Linux experience," *IEEE Security & Privacy*, 2(6):28-33, Nov.-Dec. 2004.

[Sla02] "Justifying the Common Criteria Security Evaluation," discussion thread on Slashdot website, November 2002, Accessed May 1, 2008, http://it.slashdot.org/article.pl?sid=02/11/17/2343231.

[Sow96] Sowell, T., *The Vision of the Anointed: Self-Congratulation as a Basis for Social Policy*, Basic Books, 1996.

[Spa03] Spafford, E., "Exploring Common Criteria: Can it Ensure that the Federal Government Gets Needed Security in Software?", Testimony before the House Government Reform Committee, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, CERIAS website, September 17, 2003, Accessed May 1, 2008, http://homes.cerias.purdue.edu/~spaf/usgov/tipirc.pdf.

[Sto05] Stoneburner, G., "Developer-focused assurance requirements," *Computer*, 38(7):91-93, July 2005.

[Syn] Syntegra (on behalf of the Common Criteria Implementation Board). "Common Criteria: An Introduction," CCEVS website, n.d. (1999 or later), Accessed May 1, 2008, http://www.niap-ccevs.org/cc-scheme/cc_docs/cc_introduction-v2.pdf.

[VWW02] Vetterling, M., G. Wimmel, and A.Wisspeintner, "Secure Systems Development Based on the Common Criteria: The PalME Project," *ACM SIGSOFT Software Engineering Notes*, 27(6):129-138, November 2002.

[Wai06] Wait, P., "Energy contract stirs conflict," *Government Computer News*, May 15, 2006. http://www.gcn.com/print/25_12/40754-1.html.

[Whe06] Wheeler, D., "Free-Libre / Open Source Software (FLOSS) and Software Assurance / Software Security," David A. Wheeler's website, December 11, 2006, Accessed May 1, 2008, http://www.dwheeler.com.

[Yui08] Yuill, J., "Choosing System Security-Engineering Practices : evaluation criteria and a selected survey," Technical report, 2008, https://jimyuill.com/.

About the author: Jim Yuill has over 20 years of experience in computer systems R&D. He has a PhD in computer science, with a thesis in computer security, from North Carolina State University (2006). https://jimyuill.com/