June 2011

Common Criteria

EMBRACE, REFORM, EXTEND

Presented by:

intel

cisco

Executive Summary

Common Criteria – Embrace, Reform, Extend

Discussion Draft 1.0

The security of information and communications technology (ICT) systems is an important issue for governments and companies around the world. Increasingly, organizations are searching for a mechanism to assess the security robustness of the hardware and software included in these systems. Much of this hardware and software is sold globally and makes up the global digital infrastructure (GDI). Much of the GDI is based on international technology standards with only modest variations for individual countries and geographies, and, therefore, innovators everywhere have access to global markets for their ICT products. Access to global markets increases the total available market, and increases investment in innovation. Therefore, it is important that requirements for assessing the security assurance of ICT products use a process that provides internationally harmonized evaluations standards and promotes efficiency and value.

Common Criteria (CC) is currently the only internationally recognized product assurance evaluation and certification scheme for hardware, firmware, and software. Common Criteria allows for mutual recognition by twenty six countries of the certifications provided by authorized independent laboratories through the Common Criteria Recognition Arrangement (CCRA). There are many important benefits to CC:

1. CC is a standard developed by the International Standards Organization (ISO) (15408) and embodied in a mutual recognition arrangement that includes most developed economies. The mutual recognition arrangement of CC has unified a number of different national assurance approaches to provide mutual recognition of vendors' product evaluations.
2. CC has been in use for more than a decade and thus is understood by stakeholders in the vendor community who have worked with the certification labs and schemes over time.
3. CC addresses legitimate security needs, including product assurance, without undermining the ability to develop and source products on a global scale. The ability to do a single evaluation that is accepted in many countries enables global markets and fair competition for vendors while reducing their burden and costs.
4. CC is scalable to many different types of products and fulfills many different requirements for security assurance.
5. CC provides a structured review process for developing more secure products that incorporates sufficient flexibility to address new and emerging threats.

While there are many benefits to Common Criteria, there a number of challenges and issues that cause critics to call into question its effectiveness. Some of the more heavily cited criticisms include:

- The value derived from CC does not warrant the cost (time and money). In some cases even minor changes to the product result in costly recertification which often results in only earlier versions of the product with the certification.

- CC is a lengthy and bureaucratic process that can impact product lifecycles and time to market for vendors' products. In many cases it does not complement the lifecycle of the product which can often result in significantly increased time and cost and deter vendors from certifying.
- CC often lacks consistent objective results across evaluating laboratories.
- CC process is heavily weighted to favor government needs and expectations and lacks a sufficiently transparent governance process to represent all stakeholders (vendors, laboratories, and national schemes).

To adequately address today's ICT environment, there are improvements which need to be made to modernize and reform the CC system to increase its already significant benefits. As discussed in detail below, this paper recommends the following actions:

1. Use the Common Criteria Forum (CCF) organization to drive mutual recognition and reduce or eliminate the need for geography specific certification which will in turn reduce cost to vendors from having to certify the same product in multiple geographies and allow vendors to more rapidly deliver the assurance and certifications that customers demand.
2. Establish and work through Technical Communities to develop new Protection Profiles to drive mutual recognition of certified products.
3. Accelerate and enhance Protection Profile development, through a community led process, to cover the needed product categories and enhance mutual recognition of certifications across participating schemes.
4. Improve the consistency and efficiency of evaluations to drive increased value in the certification and more trust and confidence in certified products.
5. Expand CC to address manufacturing process integrity aspects of the supply chain.

Technology vendors and their customers face an increasingly complex threat environment and a greater need to drive trust and confidence in how products are designed, developed, manufactured and distributed. To date, CC has played an important role in testing and validating products for security. However, given the increased need, CC must evolve to new and innovative models for providing trust and confidence in technology.

Common Criteria – Embrace, Reform, Extend

Discussion Draft 1.0

I. Introduction

The security of information and communications technology (ICT) systems is an important issue for governments and companies around the world. Increasingly, organizations are searching for a mechanism to assess the security robustness of the hardware and software included in these systems. Much of this hardware and software is sold globally and makes up the global digital infrastructure (GDI). Much of the GDI is based on international standards with only modest variations for individual countries and geographies, and, therefore, innovators everywhere have access to global markets for their products. Access to global markets increases the total available market, and increases investment in innovation. This innovation has? driven the development of new security features and functionality. Therefore, it is important that requirements for assessing the security assurance of ICT products use a process that provides internationally harmonized evaluations standards and promotes efficiency and reasonable value.

Common Criteria (CC) is currently the only internationally recognized security evaluation and certification scheme for hardware, firmware, and software. CC allows for mutual recognition by twenty six countries of the certifications provided by authorized independent authorities. There are improvements which need to be made to the CC system, and considerable work on these changes is underway. This work is critical as CC continues to provide the best alternative to country specific security standards and certifications. A security assurance environment which features a patchwork of country specific certification requirements will create substantial uncertainty and cost in the ICT development process. For these reasons, government and industry need to invest in CC reform. This paper explores the needed reforms of CC, evaluates current work that is underway, and proposes a comprehensive reform agenda that government and industry should urgently undertake.

II. What is is Common Criteria?

Common Criteria is a common language that allows the evaluation of security features and assurance parameters of technology products. These ICT products include hardware, firmware and software. The evaluation process tests the security functionality of a given ICT product and whether the assurance measures applied to these products meet specific requirements. The Common Criteria Recognition Arrangement (CCRA) is the multilateral agreement that provides for mutual recognition of evaluated products by participating governments. Products are evaluated by competent and independently licensed laboratories. Certificates for evaluated products can be issued by a number of Certificate Authorizing Schemes. In the context of CC, a "scheme" refers to the certificate authorizing authority in a given country. Certifications are based on the result of the evaluations and the resulting certificate is recognized by signatories of the CCRA. Four important concepts are fundamental to understanding CC evaluations.

- What will be evaluated?
  - This is known in the CC as the *Target of Evaluation (TOE)*[1]*.* A TOE can be a set of software, firmware and/or hardware.

[1] The TOE may be an ICT product, a part of an ICT product, a set of ICT products, a unique technology that may never be made into a product, or a combination of these.

- What requirements (functional and assurance) are there for evaluating a given TOE *independent* of the implementation environment[2] that the TOE will be deployed in?
    - These requirements are detailed in documents known as *Protection Profiles (PP).*
- How is the implementation environment accounted for in the CC?
    - Requirements that provide implementation-dependent statements of security needs for a specifically identified TOE are provided in a document known as a *Security Target (ST).*[3]
- How will the independent lab evaluate the product?
    - The Common Evaluation Methodology (CEM)[4] describes the minimum actions to be deployed by the independent lab when evaluating the TOE.

Common Criteria is currently recognized by twenty-six countries. The CCRA seeks to advance key objectives[5] to create an environment in which ICT products that earn a CC certificate can be procured and used without the need for further evaluation. Participating countries may be producers of evaluation certificates, consumers of evaluation certificates, or both. Certificate consuming countries use CC certified products but do not carry out CC evaluations. Certificate authorizing countries are the sponsors of compliant certifying bodies *(i.e., independent laboratories)* operating within their borders. These laboratories are able to evaluate the products and provide evidence of compliance to the national scheme that then certifies the product. . Certificate authorizing countries which have organizations or government agencies containing the resources (people, infrastructure and budget) and technical security expertise of a compliant certifying body are defined as Qualified Participants*;* they thus have final certificate issuing authority. In many countries, this responsibility resides within a national security organization or an IT or telecommunications ministry.[6]

Of the twenty-six countries that recognize the CC, fifteen countries have certificate issuing authority through independent laboratories where testing and evaluation can be completed by the certified laboratory. Upon a country's accession to the CCRA, a process exists for a country to graduate to the status of a certificate authorizing country. Upon completion of testing and evaluation by the laboratory, results are sent to the national scheme for final approval and the issuing of a certificate. It is in the purview of each sovereign country to determine which government entity is party to the CCRA. Another aspect of mutual recognition that is important to CC is the existence of a web portal to provide information on the status of the CCRA, the CC and the certification schemes, licensed laboratories, certified products and related information, news and events. The portal includes a comprehensive database of all CC evaluated products.

[2] Implementation environment refers to the larger system, network or technical environment where the product will be used.

[3] A Security Target is the document that identifies the security *properties* of the target of evaluation. It may refer to one or more PPs. The TOE is evaluated against the SFRs (see below) established in its ST, no more and no less. This allows vendors to tailor the evaluation to accurately match the intended capabilities of their product.

[4] 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 (lab) in order to conduct a CC evaluation, using the criteria and evaluation evidence defined in the CC. The CEM does not define evaluator actions for certain high assurance CC components, where there is as yet no generally agreed guidance.

[5]The objectives in the CCRA are as follows http://www.commoncriteriaportal.org/files/operatingprocedures/cc-recarrange.pdf :
a) to ensure that *evaluations* of *Information Technology (IT) products* and *protection profiles* are
performed to high and consistent standards, and are seen to contribute significantly to
confidence in the security of those products and profiles;
b) to improve the availability of evaluated, security-enhanced IT products and protection profiles;
c) to eliminate the burden of duplicating evaluations of IT products and protection profiles;
d) to continuously improve the efficiency and cost-effectiveness of the evaluation and *certification/validation*1 process for IT products and protection profiles.

[6] A comprehensive list of CCRA members is available at http://www.commoncriteriaportal.org/ccra/members/

III. The importance of Common Criteria

The current CC evaluation system plays an important role in demonstrating assurance and protecting government networks and national security interests. While both governments and vendors have identified potential CC reforms, there are many important benefits to the CC:

1. CC is a standard developed by the International Standards Organization (ISO) (15408) and embodied in a mutual recognition arrangement that includes most developed economies. The mutual recognition arrangement of CC has unified a number of different national assurance approaches to provide mutual recognition of vendors' product evaluations.
2. CC has been in use for more than a decade and thus is understood by stakeholders in the vendor community who have worked with the certification over time. This experience and longevity provides a level of certainty and consistency in the CC.
3. CC addresses legitimate security needs, including product assurance, without undermining the ability to develop and source products on a global scale. The ability to do a single evaluation that is accepted in many countries enables global markets and fair competition for vendors while reducing their burden and costs.
4. CC is scalable to many different types of products and fulfill smany different requirements for security assurance.
5. CC provides a structured review process for developing more secure products that incorporates sufficient flexibility to address new and emerging threats.

IV. Current challenges and goals for reform

While there are many benefits to Common Criteria, there are numerous challenges and issues that cause critics to call into question its effectiveness. Some of the more heavily cited criticisms include:

1. The value derived from CC does not warrant the cost (time and money). In some cases even minor changes to the product result in costly recertification which often results in only earlier versions of the product with the certification.
2. CC is a lengthy and bureaucratic process that can impact product lifecycles and time to market for vendors' products. In many cases it does not complement the lifecycle of the product which can often result in significantly increased time and cost and deter vendors from certifying.
3. CC often lacks consistent objective results across evaluating laboratories.
4. CC process is heavily weighted to favor government needs and expectations and lacks a sufficiently transparent governance process to represent all stakeholders (vendors, laboratories, and national schemes).

While these are legitimate criticisms, we believe they can all be addressed through improved cooperation between members of the CC community (vendors, labs and national schemes) to accomplish the following goals for reform:

1. Address value of certifying including issues such as time to market and patching that deter vendor certification and customer adoption of CC evaluated products.
2. Decrease risks of geography specific certification systems that would require multiple certifications for the same product by ensuring and expanding mutual recognition.

3. Increase the security value from the CC certification by broadening the consuming community.
4. Address the need for objective testing and validation criteria.
5. Provide flexibility for products with different lifecycle and build models (e.g., hardware).

V. Recommendations for achieving reform goals

While third party evaluations like CC will always result in some incremental cost (time and money), we believe that the following recommendations can increase the value of CC and provide and promote more robust products in the ICT marketplace.

1. Use the Common Criteria Forum (CCF) organization to drive mutual recognition and reduce or eliminate the need for geography specific certification which will in turn reduce cost to vendors from having to certify the same product in multiple geographies and allow vendors to more rapidly deliver the assurance and certifications that customers demand.
2. Establish and work through Technical Communities to develop new Protection Profiles to drive mutual recognition of certified products.
3. Accelerate and enhance Protection Profile development, through a community led process, to cover the needed product categories and enhance mutual recognition of certifications across participating schemes.
4. Improve the consistency and efficiency of evaluations to drive increased value in the certification and more trust and confidence in certified products.
5. Expand CC to address manufacturing process integrity aspects of the supply chain.

What follows is more detail on these five recommendations.

a. The Common Criteria Forum (CCF)

Key to the success of CC improvement will be the creation of an organization that is essentially a standards body to ensure the reform goals are met. The recently created Common Criteria Forum (CCF) should be that organization. The CCF brings together all stakeholders in the CC community including vendors, labs and national schemes. To ensure the effectiveness and credibility of the CCF, a governance process must be implemented to insure the principles of an open standard are followed, specifically:

- Fair
  - Decisions are made based through consensus based voting rules equally weighted for each participant
  - Established and predictable process and rules
- Participatory
  - Membership is clearly defined to vendors, labs and national schemes
  - All members have access to resources and due process
  - All members have the right to participate, beginning at the earliest stages, in the standards process
- Transparent
  - Decisions are transparent
  - Standards process has integrity
  - Standards process is predictable as defined by a well formed process
- Impartial
  - Guaranteed fairness through process, neutral hosting

    - Equal weighing across membership
- Available
    - Resources are readily available (drafts, work products, specifications, etc.)
    - Resulting standards must be reasonably implementable, consumable and affordable for all members
- Clear/Complete
    - Standards must be well formed, complete, well documented and the process must be predictable

b. Establish and work through Common Criteria Technical Communities

Because of the diversity of the ICT marketplace, it makes sense for those interested in working together to address issues of concern to be organized into technical communities that focus on a specific product category. Such an approach ensures that competent entities are working on the issues they are most familiar with, while providing a structure that allows the overall ICT community to scale to respond in an effective and efficient manner. A proposed initial set of communities includes the following:

Routing and switching	Data Center	Unified Communications
Wireless	Network Management	Smart Card
Operating Systems	Peripherals	Supply chain (hardware and software)
General Purpose Hardware	Web applications	Security technologies (Firewall, VPN, Intrusion Prevention Systems)

These communities should use open and transparent processes for developing Protection Profiles (PP), a document that identifies security requirements for a class of products, with participation from all stakeholders to promote mutual recognition of the PPs across national schemes. These communities will be open to all interested parties and should strive to be global in nature. The end goal is to have a growing set of PPs that are as objective as possible and that are recognized by all CCRA member countries. The mutual recognition of PPs will address cross border concerns and reduce or eliminate the need for geographically specific products or to have multiple evaluations done against the same product. It is important that these protection profiles are reflective of international customer security needs. We envision that the CCF will serve as a forum for hosting technical communities around specific technologies or issues in order to develop PPs.

c. Accelerate and enhance Protection Profile (PP) development

Customers want assurance that the ICT products they buy meet their security expectations. Certified products should give them greater assurance that the products have the required security functionality they need and that they will remain robust in a given threat environment. Properly developed and vetted PPs will help ensure that products certified against them will meet customers' needs. The aforementioned technical communities should be responsible for developing PPs. PPs are vitally important to the reform of CC because they describe implementation independent requirements for evaluating a TOE. This means that the requirements can be objective and, therefore, can be tested with reasonable certainty of the same outcome in any lab, regardless of geography. This is a key requirement for mutual recognition of an evaluated product's certificate. In recent years, vendors have used STs to define criteria for evaluation that is specific to their product. The STs have allowed a vendor to draw very specific boundaries around what should and should not be evaluated. Over time, this has decreased the importance of PPs, created confusion among customers, and contributed to an erosion of the mutual recognition of evaluated products because of the subjective nature of STs.

In the past, government schemes have had a heavy, and sometimes exclusive, hand in developing PPs which has not only slowed the process of developing PPs but also resulted in requirements incompatible with vendors' products and processes. Because the US national scheme, the National Information Assurance Partnership (NIAP), has recently issued new policies for CC evaluations[7] that rely on technical communities developing PPs, there is a need to accelerate the speed at which PPs are developed and available for use by vendors in the marketplace. We believe the technical communities can help accelerate this process if the national schemes are properly resourced for participating throughout the PP development process. This participation is critical to ensure the end product is acceptable to the largest number of CCRA members.

In addition to accelerating the rate of PP development, PPs need to be enhanced in several ways. First, they need to focus less on evaluation "levels" and more on objective, measurable criteria that can be evaluated repeatedly against different products in the same product category. For example, an operating system is a product category against which multiple operating systems (Windows, Linux, Apple) could be evaluated. NIAP is working to achieve this by rewriting all existing PPs (while also establishing technical communities to develop new ones). For this strategy to be successful there must be significant diplomatic outreach to demonstrate to all CCRA members the long term security improvements that are achievable in this model. Second, the PPs need to evaluate security functionality as well as enhance the security assurance requirements. This can be accomplished by incorporating threat models directly in the PPs. Finally, customers, especially government customers, need to demonstrate a preference for CC evaluated products in purchasing and procurement requirements. It is not adequate to have only a handful of CCRA members requiring evaluated products – all members should have such policies in place. Otherwise, vendors will not be incentivized to certify and member governments will not derive value from CC and as a result may turn to solutions like country specific certification that are not as effective or scalable as the CC.

d. Improve Evaluation Efficacy

Certified products should be more trustworthy than those that are not certified. Customers need assurance that the vendor development processes protect against today's emerging threats. At the same time, vendors operate in a very competitive marketplace and must release new technologies at a pace that the marketplace demands. Improving the efficiency of CC evaluations could result in shorter evaluation times thus addressing vendors' needs for the timely release of products and helping to ensure customers have more timely access to the state-of-the-art technologies. This will help to increase the value of CC and make the cost of certification more acceptable in

[7] http://www.niap-ccevs.org/cc_docs/CC_Community_Paper_10_Jan_2011.pdf

the marketplace. The following is a non-inclusive list of opportunities to improve the efficiency of CC evaluations:

1. A practical mechanism to leverage evaluation results from one product version to the next and across products using shared development processes will reduce the time and effort for evaluations.
2. Eliminating duplicated evaluation effort by leveraging other standards (e.g. ISO systems engineering, formal cryptographic validation, secure content automation protocol) so that efforts that vendors have already made to achieve those certifications can be obtained as "credit" in a CC evaluation.
3. Increasing the leverage across evaluations by examining and enhancing mechanisms such as: assurance continuity[8], site certification, and predictive assurance will further improve the timely delivery of state-of-the-art technologies to customers.

Finally, the Common Evaluation Methodology (CEM)[9] must evolve from a single document to evaluate all products in CC to a set of evaluation methodologies for each product category in the CC. It has become clear over time that it is unreasonable to expect one evaluation methodology to suffice for all products in CC. While efforts in the past have attempted to revise and change the CEM, they have been unsuccessful to date.

e. Expand CC to address manufacturing process integrity aspects of supply chain

We believe that CC is sufficiently flexible in its current form to address emerging challenges to security. One important example is supply chain security. While this term is often inadequately defined, we believe that the public debate around supply chain encompasses two broad areas:

1. Product Assurance[10] – this has been the focus of CC
2. Manufacturing Process Integrity[11] – this is an area that CC must expand to address

By expanding CC to address manufacturing process integrity, the ICT community is able to leverage the existing benefits of CC while expanding it make it more relevant to a broader community. The Smart Card community in the CC has made important strides to address these issues in their CC evaluations through their efforts to address manufacturing? site certification. This effort examines the policies and processes in place at a vendor's site and provides a certification of that site. This is a model that can be leveraged to address supply chain concerns in the broader CC certification process.

[8] The purpose of assurance continuity is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner.

[9] 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 (lab) in order to conduct a CC evaluation, using the criteria and evaluation evidence defined in the CC. The CEM does not define evaluator actions for certain high assurance CC components, where there is as yet no generally agreed guidance.

[10] Assurance refers to the grounds for confidence that an entity meets its relevant needs goals or objectives (corporate, standards or regulatory), for safety, security and dependability or other characteristics deemed to be critical, and possesses the related required properties." (ISO/IEC 15026)

[11] For the purposes of this paper, Manufacturing Process Integrity refers to the processes and standards used in IT manufacturing to ensure the end product conforms to the intended design parameters.

I. Next steps/Call to action

The goals described above for CC reform are achievable *if* vendors **and** national schemes commit adequate time and resources to aggressively advance a reform agenda. We believe this requires a fundamental commitment to the future of the CC on the part of both parties to realize them in the short and long-term. To begin, the following three concrete actions are needed:

1. Vendors and national schemes must prioritize and designate resources for developing PPs in technical communities and push to publish mutually recognized PPs within 6-8 months
2. National schemes must recognize the importance of CC in their national policies and refrain from creates overlapping, redundant or competing certifications.
3. Vendors and national schemes must conduct outreach globally, to the existing CCRA members and beyond, to drive consensus in a consistent and comprehensive reform agenda.[12]

II. Conclusion

Technology vendors and their customers face an increasingly complex threat environment and a greater need to drive trust and confidence in how products are designed, developed, manufactured and distributed. To date, CC has played an important role in testing and validating products for security. However, given the increased need, CC must evolve to new and innovative models for providing trust and confidence in technology.

Countries around the world are defining their own evaluation and certification processes for products. As with the proliferation of country-specific product certification schemes, this creates a burden on vendors and, could result in the unintended effect of actually resulting in less secure products. By making CC relevant for countries globally, the ICT sector can continue to provide the next generation of innovation while meeting customer requirements for functionality and security assurance.

Embracing, extending and reforming the CC will help to increase the value derived from evaluation and mutual recognition, increase certainty and consistency, facilitate international trade, enhance security assurance and create market access opportunities. Additionally, providing greater cost and time efficiency around evaluations will yield a longer effective sales life for evaluated products.

[12] We offer this agenda as a starting point and we recognize that experts throughout the CC community can enhance this proposal.