Collaborative Protection Profiles

The Benefits of an Evolved Common Criteria Implementation

September 2014

Contents

Executive Summary

Stakeholders in government and critical infrastructure sectors around the globe are increasingly looking for certified Information and Communication Technology (ICT) products that will meet their security needs.

At the same time, for ICT products to effectively defend against today's top security threats, an open community-based approach with all international participants recognizing Common Criteria is needed.

For over 15 years Common Criteria (CC) has been the leading international security certification standard for acquirers looking for validated security features of ICT products. Since its development by the governments of Canada, France, Germany, the Netherlands, the United Kingdom, and the United States, the number of participant nations has quadrupled and continues to increase –a resounding indication to the need and dependence on CC worldwide.

This paper introduces Common Criteria and provides insight into collaborative Protection Profiles (cPPs) developed by international Technical Communities (iTCs). cPPs, along with the revised Common Criteria Recognition Arrangement (CCRA), evolve Common Criteria to ensure certifications are more relevant, effective, and accepted for meeting security and procurement requirements worldwide.

Common Criteria – Introduction

The Common Criteria is a multi-part international standard for expressing security requirements along with common assurance measures and methodology for determining the claimed functionality of an ICT product is sufficient for it to meet its security objectives. Conceptually it is a framework where:

- Vendors make security claims about their ICT product.
- Certified testing laboratories/facilities evaluate the ICT product to determine if the vendor's implementation actually meets the security claims.
- End-users look for evaluation results that match their requirements – typically in the procurement process.

Key Terms and Concepts

A *Protection Profile (PP)* expresses an implementation-independent set of security objectives for a type or category of ICT product. It also specifies the security requirements and assurance measures which fulfill those objectives.

A *Security Target (ST)* expresses security objectives of a specific ICT product and defines the functional requirements and assurance measures to fulfill those stated objectives. It also defines an implementation of the security requirements. The ST forms the basis for an evaluation and may claim conformance to one or more PPs.

The *CC standard documentation* set is identified and briefly described below:

- CC standard Part 1 provides an introduction and background to the CC model.

- CC standard Part 2 presents security requirements in distinct categories of behavior.
- CC standard Part 3 presents assurance requirements which are the basis for gaining confidence the claimed security measures are effective and are implemented correctly.
- Lastly, a common methodology for evaluation processes and evaluation tasks is provided in the CEM document.

Evaluation Assurance Levels (EALs) are formed from a taxonomy of assurance classes, families, and components defined in CC standard Part 3. There are seven hierarchically ordered EALs increasing in assurance that serve to provide general-purpose assurance packages.

A Participant Nation is a government organization or government agency representing a CCRA signatory nation.

Common Criteria Recognition Arrangement (CCRA) is an agreement signed by each participant nation. By signing the CCRA, a nation recognizes Common Criteria evaluations performed by other CCRA participant nations. CCRA membership falls into two categories: authorizing and consuming:

> *An authorizing nation* sponsors and oversees an evaluation scheme and authorizes the CC certificates that are issued. An *evaluation scheme* provides the regulatory and administrative framework for laboratories or facilities within the authorizing nation to evaluate and certify ICT products.
>
> *A consuming nation* agrees to recognize ICT products certified by other authorizing nations. An authorizing nation is also a consuming nation.

The Common Criteria infrastructure includes a Management Committee and a Development Board:

> The *Common Criteria Management Committee (CCMC)* is responsible for the management of the CCRA.
>
> The *Common Criteria Development Board (CCDB)* manages the technical aspects of the CCRA, including development and maintenance of the Common Criteria standard and its associated methodology. The CCDB is also responsible for the development of cPP s by iTC s, and for providing technical advice and recommendations to the CCMC.

Common Criteria – Brief History

Prior to CC nations relied upon pre-existing criteria standards for evaluating the security of ICT products:

> ITSEC – The European standard, developed in the early 1990s by France, Germany, the Netherlands and the UK.
>
> CTCPEC – The Canadian standard followed from the US DoD standard.
>
> TCSEC – The United States Department of Defense DoD 5200.28 Std, called the Orange Book and parts of the Rainbow Series.

In the late 1990's the Common Criteria standard was produced by unifying the pre-existing standards[1]. The first major CC release came in May 1998 with the release of CC 2.0 followed by version 2.1 in August 1999. CC parts 1-3 became an International Organization for Standardization (ISO) standard in 1999 (ISO/IEC 15408) followed by the CEM which became an ISO standard (ISO/IEC 18045) in 2005.

The development of a unified Common Criteria standard paved the way for the Common Criteria Recognition Arrangement (CCRA). The aim of the CCRA was to eliminate the need for costly security evaluations in more than one nation by establishment of mutual recognition of evaluated ICT products at EALs 1-4 by all nations that officially sign onto the CCRA.

In 2007 the next significant version of the CC standard, version 3.1 was released. The current version is CC v3.1 release 4.

Statistics provided by the CC international portal as of September 2014 list a grand total of 2,436 products have been certified using the Common Criteria standard.

Improvements Collaborative Protection Profiles (cPPs) Address in CC

While there are many important benefits to Common Criteria areas exist where improvement was needed.

1. Twenty-six nations are now signatories to the CCRA. A nation recognizing evaluations performed by other CCRA participant nations has limitations. Certificate recognition means the evaluation scheme in the certificate authorizing nation correctly performed all of the activities involved in CC and CCRA processes. This does not mean the certified ICT product met the security requirements of another CCRA participant nation.

2. The requirements in the CC standard were written to be sufficiently flexible to allow specification of a wide range of ICT products. This was shown to have had an unintended effect of yielding varying and/or subjective results especially at EALs above level 2. For example, evaluation results at EAL 4 from a laboratory testing a firewall in one evaluation scheme is very difficult to compare with results produced from an evaluation laboratory in another scheme.

3. The CC was devised to ensure the evaluation fulfills the need of multiple target audiences but of particular importance is the end-user (or consumer). Product evaluations with an EAL assurance level typically claim security requirements asymmetrically from one another as a common minimum bar technologies need to meet is not defined in CC. This leaves the end-user wrestling with the arduous task of finding certified ICT products that will meet their security needs. End-users need to be made aware they have a voice in the process to collaborate on the validated security features in a technology that will meet their minimum risk tolerance.

[1] The US Federal Criteria was an early attempt to combine these other criteria with the TCSEC.

Another end-user complaint is the evaluation process takes too long while product vendors often say the evaluation costs are too high. Industry changes that bring new vendor technologies, product development approaches, and shorter time to market serve to exacerbate these problems.

To address these needed improvements, the CCRA Management Committee (CCMC) announced in September 2012 a shift away from harmonizing the CC/CEM processes among the divergent and growing evaluation schemes to instead focus on development of new-style Protection Profiles called *collaborative Protection Profiles* or cPPs. cPPs are developed by *International Technical Communities* or iTCs. cPPs move away from Protection Profiles of the past that were developed without strong engagement and endorsement of all CCRA participant nations.

iTCs and cPPs: Defining Common Minimum Requirements for Technologies

International Technical Communities (iTC)

An iTC is a structure to discuss and agree upfront on what are the common minimum security requirements and reasonable assurance measures for a technology to defend the top-level threats it faces. Rather than establishing criteria standards in closed-door government settings, iTCs bring in an open international forum the skills, expertise, and security knowledge from all stakeholders in the evaluation.

iTCs are composed of but not limited to:

- Scheme experts
- Product vendors
- Consultants and Evaluators
- Government end-users

Collaborative Protection Profiles (cPPs)

International Technical Communities (iTCs) create and maintain collaborative Protection Profiles (cPPs) and associated supporting documentation for technologies that are of national interest to CCRA participant nations.

Once duly authorized by the CCDB, iTCs will use the framework of the CC standard (ISO/IEC 15408) to develop cPPs that contain the minimum set of common security functional requirements for the technology type.

Rather than using general-purpose security assurance packages predefined in an EAL structure, iTCs will utilize the taxonomy of assurance classes, families, and components defined in the CC standard to create a cPP with an achievable level of assurance tailored where necessary to the technology type. This will result in a level of assurance that will repeatable and comparable among evaluation laboratories and facilities in any certifying scheme.

When an iTC has finalized a cPP, participant CCRA nations will issue public endorsement statements of the cPP for which their government has a national requirement. Additionally, participant nations can declare how the cPP is linked to their policy on procurement.

Lastly, by evaluating an ICT product against a published cPP, authorized laboratories and facilities can focus their activities on areas that are of most concern to the iTC participants, resulting in reduced cost and length of time required for an evaluation.

CCRA Revision

The changes in the revised CCRA will permit mutual recognition, in all participant CCRA nations, ICT products that are evaluated against a cPP.

After a transition period cPPs will be applied instead of ICT products evaluated with an EAL assurance level. The revised CCRA will only permit an evaluation with an EAL assurance level for cases where a cPP does not exist for the technology or is not applicable. CC certifications where a cPP does not exist or is not applicable will be mutually recognized only at or below EAL 2.

Summary - An Evolved CC Benefiting All Stakeholders

cPPs that focus evaluation testing on the security threats that are of most concern to stakeholders produces evaluation results that are reasonable, comparable, relevant, and cost-effective.

Incorporating the security requirements of CCRA participant nations into the cPP produces more meaningful and useful evaluation results.   The mutual recognition of a CC certificate is strengthened and tied to procurement policies for those nations that have national requirements for the technology. This increases the global market value of the Common Criteria for all stakeholders and ensures certified ICT products reach a worldwide common-level of security assurance where product vendors can evaluate their product once and truly meet security and procurement requirements worldwide.

The benefits of an evolved CC implementation outlined in this paper are summarized below:

1. *Relevant – iTC to develop, maintain, and update collaborative protection profiles that meet the security concerns of end-user.*
2. *Recognized - Security requirements appropriate to end-user needs and differing technologies that are recognized across 26 nations.*
3. *Repeatable – Evaluation results that are comparable and reproducible.*
4. *Reviewed – Authorized laboratories or facilities provide independent review to ensure the product performs as designed/advertised.*
5. *Reasonable – Timely evaluations ensure end-users get evaluated products shortly after general release.*
6. *Revealing – Requirements are developed transparently in open and collaborative technical communities.*

For More Information and How to Get Involved

1. Contact your local scheme. Web sites and contact information for all CC schemes can be found on the International Common Criteria Portal at:
   http://www.commoncriteriaportal.org/ccra/members/

2. To locate information on International Technical Communities that are developing collaborative Protection Profiles (including invitation letters describing how to join) refer to:
   http://www.commoncriteriaportal.org/communities/

3. Join the Common Criteria Users Forum (CCUF) at http://www.ccusersforum.org/
   The Common Criteria User Forum mission is to provide a voice and communications channel amongst the CC community including the vendors, consultants, testing laboratories, Common Criteria organizational committees, national schemes, policy makers, and other interested parties.