Introduction to Common Criteria
(Step One in Information Survivability)

Short Talk, with FAQs

By
Dr Jean-Guy Rioux, Jr. CD, CGEIT, PMP
TUV Rheinland Japan
CCEL Manager

CCS Overview

- The Common Criteria Evaluation and Certification Scheme, or CCS for short, is a independent 3rd party evaluation and government certification (validation) service for measuring the security assurance and functionality claims (trustworthiness) of Information and Communications Technology (ICT) products and systems

What you need

- As an IT customer (end-user):
  - You need reliable, tested IT products that are secure from a growing number of system and network threats - and you need them sooner, rather than later

What you need

- As an IT software developer (vendor):
  - You need a fast track for proving the security of your products, not just in India, but in all major markets as well.

What you need

- As an IT security specialist (consultant):
  - You need opportunities; niches where you can serve the market, helping it - and you - grow and prosper.

What you need

- Fortunately, for all three sectors - IT customers, vendors/manufacturers, and IT security specialists, the Government of India, along with 23 other countries, has initiated a program to meet your collective needs by establishing the Common Criteria Evaluation and Certification Scheme (CCS).

Background

- In the early 1990s, the Governments in Canada, France, Germany, Netherlands, the United Kingdom, and the United States all came to the same conclusion: to speed the approval of much needed secured IT products – and to maximize opportunity for their vendors – the traditional "test it in each country" approach needed reform. That is why, in October 1998, the Common Criteria work became an international initiative by the following organisations: CSE (Canada), SCSSI (France), BSI (Germany), NLNCSA (Netherlands), CESG (UK), NIST (USA) and NSA (USA). They signed a Mutual Recognition Arrangement (MRA) based on the Common Criteria (CC) and Common Methodology (CEM) for IT Security Evaluation. Under the MRA, the results of a product evaluation conducted in one of these countries are automatically recognized in the others.

Background (continue)

- To accommodate countries who do not wish to provide certificates for mutual recognition, but still wish to recognize CC Certified products, the MRA was replaced by the Arrangement on the Recognition of Common Criteria Certificates (CCRA). This new arrangement allows countries to participate in the CC project as certificate producers (Australia & New Zealand, Canada, France, Germany, Japan, Republic of Korea, Netherland, Norway, Spain, Sweden, the United Kingdom, and the United States) or as certificate consumers (Austria, Czech Republic, Denmark, Finland, Greece, Hungary, India, Israel, Italy, Malaysia, Singapore, and Turkey).

Fast-tracking security testing for the world's markets

- For IT customers:
  - The CCS means faster access to IT products that are certified: something that matters in a world inhabited by hackers and other threat agents.

Fast-tracking security testing for the world's markets

- For vendors:
  - The CCS means quicker time-to-market delivery for new ITS products, less money spent on expensive tests, and access to a wider marketplace.

Fast-tracking security testing for the world's markets

- For IT security specialists:
  - The CCS offers business opportunities, namely to establish Common Criteria Evaluation Laboratories (CCEL) accredited as an IT Security Evaluation and Testing (ITSET) Facility, under ISO/IEC 17025-2005, and approved to perform CC evaluations.

How the CCS works - short version

- Under the CCS, 47 private sector CCELs have been established in 12 countries (Australia & New Zealand, Canada, France, Germany, Japan, Republic of Korea, Netherland, Norway, Spain, Sweden, the United Kingdom, and the United States).
  - Note: atsec information security, Swedish CCEL, operates in Germany, Sweden, and the United States (also in China), TÜV Informationstechnik (TUViT) operates in Germany and Japan, and secunet SwissIT, a Swiss CCEL (Switzerland is not a CCRA member), operates under the German CCS. (China and Russia adhere to the CC principles and have their own CCS, but are not CCRA members for internal reasons. Belgium recognizes CC certified IT products without CCRA membership.)

Integrity and Competence

- The integrity and competence of the CCELs is paramount:
  - users have to be able to trust that CCEL-evaluated products are as secure as they are certified to be, whether the products are made in India or elsewhere.
  - Meanwhile, manufacturers/vendors need to be able to rely on the fairness of the testing procedure, as well to be assured that their trade secrets are protected.
  - Finally, for the CCRA to function, CCEL evaluations, and the evaluation laboratories of the other CCRA partners must be unquestionably valid.

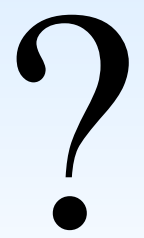
CCEL Accreditation

- This is why all aspiring CCELs must apply to and be accredited by the Government of India Department of information technology – STQC IT Services, under the Indian Information Technology Security Evaluation and Testing Facility (ITSET) Accreditation Program (ISO/IEC 17025-2005).
- Moreover, Government of India Department of Information Technology will have to establish a Certification Body (CB) to approve accredited laboratories to perform CC evaluations and to oversee the operation of the CCS and certify evaluation work – if it wishes to become a certificate approving CCS.
- It will require expertise in ensuring the security of information; India has the people and expertise to ensure that private sector CCELs deliver the full promise of CC.

Trustworthiness

- Once accredited and approved, CCELs are the catalyst that makes the CCS work.
- More then ever in the short history to Cyberspace, IT security testing need to be fast-tracked for manufacturers/vendors, so that IT users get the secured IT products they need sooner, without sacrificing quality.
- For both government and private business users, the CCS is providing for the best, quickest, and most reliable IT security solutions.

Frequently Asked Questions



FAQ

Scheme Questions

What is the benefit in having certified products and systems?

- The use of certified products and systems provides a high-level of confidence that the claims being made about security functionality have been independently verified and tested.
- It demonstrates that the vendors have faith in their product by taking the time and trouble to seek an independent evaluation of the security claims against a pre-determined level of assurance.

What is Common Criteria?

- Common Criteria (CC) represents the outcome of international efforts to align and develop the obsolescent European Information Technology Security Evaluation Criteria (ITSEC) and North American – U.S. Trusted Computer System Evaluation Criteria (TCSEC) and Canada's Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) – criteria towards a common standard for carrying out security evaluations.
  - By establishing a common base, the results of an ICT security evaluation are more meaningful to a wider audience.
- CC has a catalogue of standard Security Functional Requirements (SFRs) that represent the current state-of-the-art for trusted products and systems.
  - These can be used to develop a Protection Profile (PP) and as a means for developing a Security Target (ST).
  - They can also be supplemented or tailored to suit more specialist requirements.
- A CC evaluation is carried out against a set of pre-defined assurance levels, termed Evaluation Assurance Levels (EAL1 to EAL7).
  - This scale represents ascending levels of confidence that can be placed in the TOE Security Functions (SFs) and determines the rigor of the evaluation.

How does a CC evaluation compare to other security evaluation types?

- Most other schemes are based on black box testing concentrating on finding security errors through penetration testing.
- Common Criteria operates based on white box testing where the evaluation is subject to a more structured and formal approach.
  - The evaluator acquires an in-depth knowledge of the construction of the product by examining the required security functions and tracing the security functionality to lower levels of design or implementation.
  - In addition, depending on the assurance level, the evaluators will examine how guidance is given to administrators and users, how the product is developed, and how vulnerable the product is to attack.
    - White box testing may take longer than black box testing but more confidence can be placed in the end-results.

What is Mutual Recognition?

- Mutual Recognition is a formal arrangement whereby other participating nations agree to recognize a security certification from a qualifying Certification Body (CB).
- This helps vendors to cut their costs by having a single product or system evaluation that is recognizable by all participating nations.
- CC Certifications up to and including EAL4 are mutually recognized by Australia, Austria, Canada, The Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, The Republic of Korea, The Netherlands, New Zealand, Norway, Singapore, Spain, Sweden, Turkey, The USA and the UK.
  - CC certifications are recognized internationally, outside the MRA.

What is the Scheme Certification Mark?

- The Scheme Certification Mark demonstrates that a specific product or system has been evaluated and certified under a CC Scheme.
- Vendors who have had their product or system certified under the Scheme are authorized to use the CC Scheme Certification Mark in their literature and marketing material.

What is the role of a CC Evaluation Laboratory (CCEL)?

- A Common Criteria Evaluation Laboratory (CCEL) is an organization that is appointed by a Certification Body to conduct security evaluations in accordance with the standards of the CC Scheme.
  - Because CCELs are testing laboratories, they are regularly inspected by government agencies.
- Each CCEL is appointed to perform evaluations to the necessary standard and to a specified Assurance Level, as determined by the scope of the CC accreditation.
  - The main requirement of a CCEL is to be totally independent from the developer of a product or system, including its parent company.
- CCELs are usually contracted by sponsors of products and systems to undertake security evaluations.

Who are the CCELs and how can I get in touch with them?

- There are currently 46 Common Criteria Evaluation Laboratories (CCELs).
- They welcome enquiries from any one with an interest in evaluation.

FAQ

Purchasers Questions

Will certified products cost me more money?

- No, because the vendor pays for evaluation and this cost tend to be absorbed in research and development.

How can I tell whether a product or system fulfils my security requirements?

- A CC certificate provides assurance that a product or system has met a Security Target based on security objectives, threats, functionality and the environment in which it is intended to operate.
- In addition, the scheme's hierarchical levels of assurance allow you to match your requirements for confidence precisely against the vendor's claims.
- Therefore, the first step is to decide on what level of assurance is required (e.g. EAL3) and then to read the Security Target and Certification Report to determine if a particular product or system matches your security requirements.
- If these are unavailable, you may require a security evaluation.

Exactly what is a security evaluation?

- A security evaluation using an appropriate set of evaluation criteria and methodology is a process aimed at establishing a required level of assurance as to the absence of vulnerabilities in a Target of Evaluation (TOE).
- The higher the value of the assets requiring protection, and the greater the threat to those assets, the higher the assurance needed to reduce the residual risk to those assets to an acceptable level.
- Through evaluation, the sponsor seeks to demonstrate a level of confidence, commensurate with the identified risk, in the countermeasures provided by the TOE.
- It is the responsibility of the evaluator to confirm the required assurance, using deliverables supplied by the developer as inputs to the evaluation, and to use the knowledge gained for devising effective penetration tests

What is a TOE?

- A TOE is a well-used acronym in security evaluations and refers to the Target of Evaluation.
- The TOE is that part of the product or system which is to be subjected to evaluation, including its associated administrator and user guidance documentation.
- It may be a single component operating in isolation (e.g. a PC start-up boot process) or it may be constructed from several components which are layered together (e.g. a database management system sitting on of an operating system).

What is a Security Target?

- A Security Target is a document that forms the baseline for evaluation of a product or system (i.e. the TOE).
- It is an important input to the evaluation process and the Security Target itself is subjected to scrutiny to ensure that it is complete, accurate, and consistent.
- It contains a specification of the security functions against which the product or system will be evaluated, and includes a description of the threats and security objectives present in the environment in which the product or system is to operate.
- The audience of a Security Target is therefore not confined solely to those undertaking the evaluation, but also for those responsible for purchasing, managing, installing, configuring, and using the product or system.

What is a Protection Profile?

A Protection Profile (PP) is a document used within security evaluations under Common Criteria.

- A PP is an implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs for IT security.
- Many PPs are currently being designed to cover most aspects of application security.
- Existing examples of PPs include:
  - the Canadian Firewall PP,
  - Oracles Database Management System PP, and
  - the UK Controlled Access PP and UK Labelled Security PP.
- Each PP contains a description of the intended environment, security objectives, security functions, and assurance requirements.

What is a Protection Profile? (continues)

- A PP itself is subjected to a Common Criteria evaluation and only those that pass the evaluation are eligible for inclusion in a central registry.
- The registry is currently under construction and will be supported by a web site on the Internet.
- There are several advantages to using a PP:
  - provides guidance to developers on the state-of-the-art security requirements for a product type;
  - enables purchasers to select products and systems that are conformant to a particular requirement set; and,
  - helps sponsors to construct Security Targets more easily.

What Protection Profiles are currently available?

- Several Protection Profiles have been developed and many more are currently in production by participating nations.
- A centralized registry with a supporting web site has been constructed to hold details of all evaluated and approved Protection Profiles.
- http://www.commoncriteriaportal.org/pp.html

What are Security Functions?

- Security functions are features that are designed into a product or system at the development stage.
- They are user and administrator requirements which are needed to prevent or detect accidental/intentional misuse of the operational software.
- Security functions generally cover Confidentiality, Integrity and Availability aspects.
- Typical examples are:
  - Identification and Authentication,
  - Access Control,
  - Audit,
  - Accountability,
  - Object Re-use,
  - Accuracy,
  - Reliability of Service, and
  - Data Exchange.

What are evaluation assurance levels?

- Common Criteria and other sets of evaluation criteria operate the concept of assurance levels.
- For Common Criteria the levels are EAL1 to EAL7.
- These scales represent ascending levels of confidence that can be placed in the TOE meeting its security objectives.
- The higher the level the greater the degree of rigor is applied in assessing whether the TOE has met its security requirements (e.g. by intensifying the analysis and search for security vulnerabilities in the TOE Security Functions).

Is there a list of certified products and systems?

- An up-to-date list of Certified Products is accessible online at the CC Portal website or individual Scheme websites.
- http://www.commoncriteriaportal.org/products.html

Which documents provide details of the evaluation process?

- Access to various introductory guides and formal documentation is available via this site, and the Common Criteria website.
- http://www.commoncriteriaportal.org/thecc.html

FAQ

Vendors Questions

Why should we have our ICT product or system evaluated?

- Security now forms an important consideration in the software selection process by most commercial firms and government agencies.
- These organizations have neither the time nor resources to verify the validity of security claims to the same level as that undertaken by a skilled evaluation facility.
- There is a greater opportunity for increased sales if vendors have their security claims independently verified using an approved scheme.
- This is demonstrated by the firewall and network printer market – it is now normal practice for purchasers of these products to choose CC certified versions.

What type of product or system can I have evaluated?

- Any electronic product or system that claims to have a security capability can be evaluated e.g. - operating systems, database management systems, firewalls, communication systems, smartcards, data separators, PKI systems, e-commerce systems.
- In practice, most evaluations are usually undertaken on software components, but the field is beginning to widen to include more firmware and hardware (see Certified Products List on the Common Criteria Portal)

How much does it cost to get my product/system certified?

- The cost of evaluation can be split three ways:
  - developer cost in providing the correct documentation to the CCEL;
  - the CCEL costs in performing the evaluation itself; and,
  - the Certification Body costs in monitoring and certifying the evaluation.
- There is also a dependency on the nature and complexity of the software, the assurance level required and whether any re-use can be made of work performed from previous evaluations of the same product or system.
- All aspects of costs are confidential to the parties concerned so it is not possible to give an accurate estimate.
  - If you are considering having your product or system evaluated, both the CCEL and the CB will be pleased to provide a quote for the work involved without obligation.

Should my product undergo a CC evaluation?

- Vendors who wish to sell into Government Organizations in Europe and North America are advised to incorporate Common Criteria.

How long does evaluation take?

- Most product evaluations are completed within 6 to 12 months of starting.
  - Others, of a more complex nature, can take much longer depending on the scope of the Security Target.
- The elapsed time for the whole process is dependent on the availability of the correct developer documentation - e.g. design and operational documentation.

What evaluation documentation is required?

- For CC evaluations, the developer is required to provide at least application design and operational guidance documentation.
- CC Part 3: Security Assurance Requirements details the documentation required for CC evaluations.

How do you maintain certification for new products or systems?

- Once a product or system has been successfully evaluated, CC and the alternative approaches operate assurance maintenance methodology for maintaining certification without having to undergo separate evaluations for each new version of software.
- The concept is to ensure that a TOE continues to meet its security target as changes are made to the software or its environment.

What does a Certifier/Validator do?

- The Certification Body of the CC Scheme employs a number of Certifiers (validator) to monitor the conduct and performance of evaluations and to produce certification reports reflecting the outcome of evaluation results. In practice, this means that for each evaluation the Certifier:
  - holds a kick-off meeting with the sponsor and CCEL to confirm that the TOE is suitable and ready for evaluation (e.g. agreeing the TOE Scope, Evaluation Work Plan, timescales and the Security Target)
  - monitors the progress and performance of the evaluation, resolving concerns with the sponsor and CCEL (e.g. ensuring comprehensive testing is performed on the TOE, co-coordinating assessment work on cryptographic algorithms)
  - reviews CCEL evaluation technical reports against the evaluation criteria and methodology, and produces a Certification Report or statement agreeing the result with the sponsor and CCEL.

What consultancy services are available to sponsors?

- Sponsors of evaluations have the option of attending an informal meeting with the Certification Body to discuss which evaluation options are more suitable for their business.
- Each of the CCELs provides a consultancy service to help sponsors in the production of evaluation documents.

Whom do I talk to if I am considering evaluation?

- A good place to start is with the Certification Body (CB) itself who will be pleased to give further advice.
- You may also wish to contact one of the CCELs who will be willing to give appropriate advice.

Thank you for your attention and time