COMMON CRITERIA EVALUATIONS IN THE US: WHAT A DEVELOPER SHOULD KNOW

Kimberly S. Caplan
Douglas Stuart, CISSP

Computer Sciences Corporation
7471 Candlewood Rd
Hanover, MD 21076

Abstract

The National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme for Information Technology (IT) Security will soon be officially stood up, and be the United States' scheme for Common Criteria evaluations. The Trust Technology Assessment Program (TTAP) is currently a "proof of concept" program and, similar to the NIAP scheme, allows Common Criteria evaluations to be performed by authorized commercial laboratories. In the U.S., it is a new concept to have commercial laboratories perform security product evaluations against a criteria and to place the results of the evaluation on the Evaluated Products Lists (EPL). In the past, the Government solely performed security product evaluations under the Trusted Product Evaluation Program (TPEP). Because of the newness of the TTAP and NIAP Schemes, the responsibilities and expectations of these programs are not well understood. As an authorized TTAP lab, Computer Sciences Corporation (CSC) has answered several questions from Developers about the Common Criteria. This paper is written for the Developers of security products who are interested in pursuing an evaluation under the TTAP and NIAP Schemes. It is the authors' intention that this paper will help Developers understand Common Criteria evaluations, what investment they must be willing to make for a successful evaluation, and what they can expect in return.

Key Words: Common Criteria, ITSEC, NIAP, security product evaluations, TCSEC, TTAP, TPEP.

Introduction

This paper describes the areas of most interest to Developers of security products who want to participate in an U.S. evaluation under the TTAP and the emerging NIAP Common Criteria Evaluation and Validation Scheme for IT Security. This paper was written in response to many Developers who are struggling with the newness of the *Common Criteria for Information Technology Security Evaluation* (CC) [1] and CC evaluations, and who are determining if their product should undergo a CC evaluation. This paper captures *current* TTAP and NIAP CC Scheme processes, procedures, and policies and is based on lessons learned from experiences working with Developers on CC evaluations. Because of the influences of both the *Trusted Computer System Evaluation Criteria* (TCSEC) [2] and the *Information Technology Security Evaluation Criteria* (ITSEC) [3] to the CC, this paper will make comparisons to these documents and their supporting evaluation schemes. It should be understood that views expressed in this paper might differ from others in the evaluation and developer community. It is the authors' hope that this paper will enlighten a Developer's current knowledge about security product evaluations and give them information that will aid them to make informed cost-effective decisions.

Presentation of information

The CC is not an easy document to understand in one reading. It has been our experience that a developer has a lot of questions about CC evaluations because of the lack of simple and concise information about the CC, evaluations using the CC, and all its implications. Most of the questions asked are concerned

with time, cost, developer resources, documentation/deliverables, Protection Profile conformance, and ratings maintenance.

In order to address these areas properly, this paper first presents background information focusing on the various evaluation schemes and the evaluation process in general. Next, the paper briefly presents concepts of the CC. The remaining sections address the question areas listed above by describing what the Developer should understand about the evaluation process, details about evaluation deliverables, and the relationship with the authorized laboratory (i.e., evaluation team).

Background

Evaluation Schemes

The U.S. experience with commercial Information Technology (IT) product evaluations originates from the TPEP in which the National Security Agency (NSA) performed evaluations using the TCSEC. The primary focus of TPEP evaluations was operating systems and was later expanded to include networks and database systems. The primary benefit of TPEP evaluations was the rigor of design analysis and testing performed by the Government evaluation team such that the placement of the product on to the EPL meant a consumer had reasonable assurance that the product did satisfy the requirements of the TCSEC. These evaluations were conducted in accordance with a defined evaluation process in which the evaluation team produces an initial evaluation report and a final evaluation report and presents findings to a Technical Review Board (TRB). Once the evaluation was completed and a rating approved, the product was placed on the EPL. The major vendor criticism of TPEP evaluations is the amount of time it takes to complete an evaluation. The rating of products on the EPL quickly became obsolete due to new releases or enhancements to the products.

With the development of the CC, IT product evaluations transitioned from TPEP to TTAP. The major difference between these evaluation schemes is under TTAP the evaluations are conducted by authorized commercial laboratories. These laboratories are authorized to conduct C2 and B1 evaluations using the TCSEC and Evaluation Assurance Level (EAL) 1 through EAL 4 evaluations using the CC. TTAP is a transition program to the newly established NSA and National Institute of Standards and Technology (NIST) NIAP CC Evaluation and Validation Scheme for IT Security. The NIAP scheme will become the U.S. Scheme for CC evaluations in which certificates of CC evaluations are mutually recognized by all countries who sign the Mutual Recognition Arrangement.[1]

Another evaluation scheme is the UK IT Security Evaluation and Certification Scheme which uses the ITSEC to conduct evaluations of IT products and systems. Licensed commercial facilities conduct these evaluations. The depth and rigor of design analysis and testing is determined by the E level of assurance (E1 to E6) to evaluate the product. The facility submits a technical report describing their evaluation findings to the Certification Body who in turn publishes the evaluation results in a certification report and issues a certificate for the product, if appropriate.

Evaluation Process and Stakeholders

The major milestones/activities of an evaluation under TTAP/NIAP Schemes are shown in Figure 1. These milestones/activities are performed by or achieved by three principal players: the Developer (Sponsor), the laboratory, and the Validation Body.[2] The Developer should be thought of as the

---

[1] The Arrangement, officially known as the *Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security* was signed in October 1998 by the U.S., Canada, France, Germany and the UK.

[2] It should be noted that the exact names of these key players are referred to differently in the TTAP scheme and NIAP scheme but their roles and responsibilities are the same. The terms developer and sponsor are synonymous.

individual or organization paying for the evaluation. This could be the actual vendor of the product or a sponsoring organization. It is the Developer who negotiates a contract with a lab and pays for the evaluation. The Developer is responsible for providing all the necessary evaluation evidence. The laboratory is approved by the Validation Body to conduct evaluations. The laboratory must undergo a qualification process based on ISO Guide 25 requirements to become and sustain being an authorized lab. The qualification process is different between the TTAP and NIAP Schemes. Under TTAP, a lab becomes authorized by approval of its application package and by signing a cooperative research and development agreement. Once approved, TTAP allows the lab to conduct all types of evaluations as described by the scheme. Under NIAP, the lab must be accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP). A NIAP lab must qualify for each type of evaluation (e.g., EAL 1) separately. Under both schemes, the Validation Body monitors all evaluations. The primary objective of the Validation Body is to ensure a competent IT security evaluation scheme. Thus, the Validation Body sets the policies and procedures for all aspects of the scheme. It is the Validation Body that in the end approves the results of the evaluation and issues a certificate.

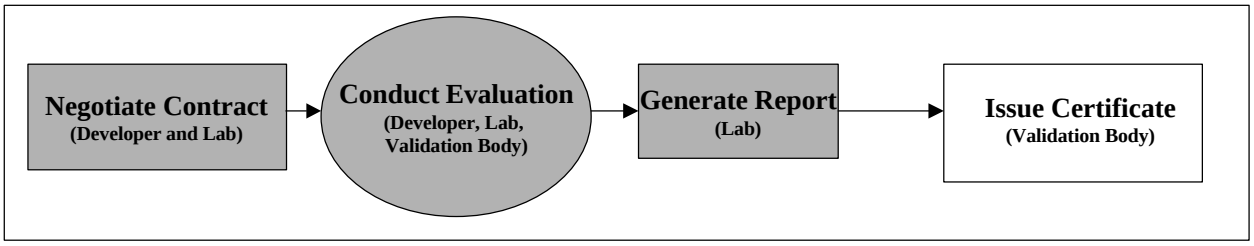

Figure 1 Evaluation Process and Participants

Understand the Common Criteria

Fundamental Concepts

The CC, presented in three parts, describes a generic set of Security Functional Requirements (SFRs), Security Assurance Requirements (SARs) and supporting information to be used as a basis to articulate and evaluate security properties for IT products and systems. Importantly, the CC advocates capturing these properties in a model that supports Protection Profiles (PPs) and Security Targets (STs). During an evaluation, the IT product or system is referred to as the Target of Evaluation (TOE). A PP is primarily used by a consumer base to state security requirements about a particular type of TOE to meet their specific needs. The PP is not meant to be implementation specific but rather reusable to define TOE security requirements that are known to be effective in meeting the TOE's security objectives. An ST is used by the Developer to identify the specific security requirements their product satisfies. The ST describes the Developer's claims of what their product offers with respect to the identified requirements. A ST is the document used for a TOE evaluation and *can* derive its requirements from a PP. The evaluator uses the ST to determine what the security functional and assurance requirements are for the TOE.

The CC describes three types of evaluations: PP, ST, and TOE. The PP and ST evaluations are carried out against evaluation criteria stated in CC part 3. The TOE evaluation is carried against the evaluation criteria as defined by the assurance requirements identified in the ST. An EAL is a predefined set of SARs for evaluation. The CC defines seven EAL packages (EAL 1 – EAL 7) which increase in depth, rigor, and evaluation evidence required. A SAR is defined by assurance elements. It is important to

understand that all the assurance elements[3] presented in Part 3 are in support of evaluations. There are three types of assurance elements: *Developer Action Elements*; *Content and Presentation of Evidence Elements*; and *Evaluator Action Elements*. The Developer is responsible for satisfying *Developer Action Elements* and *Content and Presentation of Evidence Elements* for each assurance component presented in the ST. The evaluator (lab) must conduct the evaluation according to the *Evaluator Action Elements*.

What to Know about the Common Criteria

It has been our experience that a Developer is not interested in reading a 600-page document front to back nor would it be recommended. The CC should primarily be used as reference document once an ST has been written. The ST must be written using all parts of the CC and if the Developer writes the ST, they must understand all parts. Specifically, the Developer will use:

- Part 1 Appendix C to write the ST. Part 1, Appendix C defines the mandatory content requirements for an ST;
- Part 2 to define security functional requirements; and
- Part 3 to write the ST and to define security assurance requirements. Part 3 presents the evaluation requirements for an ST evaluation as well as presents the definitions of EALs and security assurance requirements.

For a TOE evaluation, the Developer only has to understand CC Part 3 because this part explicitly states the evaluation requirements of the Developer and the evaluation team. The Developer must pay particular attention to the *Developer Action Elements* and *Content and Presentation of Evidence Elements* presented in CC Part 3 for every assurance requirement specified in the ST. It is these elements that scope the obligations of the Developer. Unlike the TPEP, the evaluator cannot request additional evidence beyond what is described within these requirements. Because the Developer has full knowledge of the boundaries of the evaluator's analysis by the *Evaluator Action Elements* of an assurance requirement, the Developer is able to challenge unreasonable requests for additional evidence. Some would argue that the developer should be knowledgeable of the CC Part 2 because SFRs are derived from this part. If the ST is a stand-alone document containing all the SFRs for the TOE, the Developer needs to understand the functional requirements in the ST versus the source of the requirements. However, the Developer may need to refer back to Part 2 Annex for guidance and interpretation.

Importance of a Protection Profile

Identifying security requirements for a TOE is one of the hardest steps a Developer will face in preparing the ST. The CC provides a framework of functional requirements and assurance requirements that must be tailored for the particular TOE. Because a Developer's primary motivation for seeking a CC evaluation is to sell a product, the requirements chosen should be inline with what functionality and assurance consumers are demanding. A PP is how Developers are informed of what matters to a consumer and provides a valuable mechanism for specifying an implementation independent set of security requirements for a type of TOE. By using a PP, the Developer is provided with a basis for producing their security target that reflects the product implementation of the security requirements defined in the PP. When the TOE is evaluated, the ST evaluation will include a conformance check to the PP and the resulting certificate for the TOE will identify conformance to a PP.[4] This identification will let consumers know which PP the TOE satisfies. It is recommended that a Developer researches whether

---

[3] Requirements in CC are presented by a family, class, component, element structure. An element is the smallest security requirement recognized in the CC.

[4] A ST can be conformant to more than one PP.

a PP is available for their type of TOE and if it can be used in developing the ST. A PP could cut the amount of effort in producing the ST because a set of security requirements for the TOE is defined.

Comparison to ITSEC

The CC has adopted many of the underlying security evaluation concepts directly from the ITSEC, most notably the inclusion of the Security Target as the basis of a product or system evaluation. It should be understood however, that an ITSEC ST is *not* the same as a CC ST. The content requirements are slightly different such that an ITSEC ST would have to be modified to satisfy the *Content and Presentation of Evidence Elements* for a ST evaluation under the CC.[5] The ITSEC addresses the concept of evaluation assurance through effectiveness and correctness of the security functions implementation. The CC has adopted all of the effectiveness and correctness assurance measures, in some form, through the set of security assurance requirements provided in Part 3 of the CC. Table 1 shows a comparison of assurance levels between the ITSEC, TCSEC and CC. Also, this comparison will help to identify what ITSEC evaluation evidence can be easily reused for a CC evaluation.

Table 1 Assurance Level Comparison

CC	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ITSEC	-	E1	E2	E3	E4	E5	E6
TCSEC	-	C1	C2/B1		B2	B3	A1

The most notable difference in the CC is the inclusion of a catalogue of security functional specification components.[6] These specifications are presented as a set of templates that can be used by a Developer to express the security functionality provided by an IT product. The ITSEC requires the Developer to define the security enforcing functions of a product from scratch with only limited guidance provided through a set of generic security function headings.

The major benefit that the CC has over the ITSEC is the facility for providing an implementation independent set of security functional requirements through a PP. The ITSEC allows the developer or sponsor to set their own set of security enforcing functions that is inevitably biased towards what the security product can do. Comparing the functionality of ITSEC evaluated products becomes difficult because the set of security enforcing functions defined for one product is not similar for another product. Under the CC paradigm, the consumer has a basis for comparing products that conform to the same PP.

Understand the Evaluation Process

Although the CC provides the requirements for the evaluator to conduct a CC evaluation, the CC does not describe the evaluation framework (scheme) or methodology by which the evaluator must conform to when applying the *Evaluator Action Elements*. The Developer should understand the evaluation milestones and phases prescribed by the scheme to monitor progress of the lab and Validation Body and to appreciate the commitment and investment that must made for a successful evaluation.

The evaluator must use the Common Evaluation Methodology (CEM) [4] when conducting an evaluation.[7] The CEM provides an agreed methodology for conducting CC evaluations and must be used

---

[5] ST evaluation requirements are defined in CC Part 3, Chapter 5.

[6] Security functional specifications are presented in CC Part 2.

[7] Under TTAP, application of the CEM is mandatory, if available.

as part of the Mutual Recognition Arrangement. Although the CEM is primarily for evaluators, the Developer could gain useful information from the CEM with regards to what the evaluator is looking for when examining evaluation evidence. The CEM provides additional information about and interpretations of the *Content and Presentation of Evidence Elements* presented in CC Part 3, which are not found in the CC.

In addition to using the CEM, the evaluation team must conduct the evaluation according to the scheme's prescribed process for technical oversight and validation. The TTAP scheme follows two evaluation processes as shown in Figure 2. Common milestones/events shared between these processes are the contractual agreement between the lab and Developer, the generation of Observation Reports (ORs), submission of a Final Evaluation Report (FER), approval of the results, and EPL posting. The main differences are the Validation Body role and what the evaluator must provide to the Validation Body at the higher EALs. The Developer should understand that because of the added oversight required at the higher EALs, the cost and time of an EAL 3 and EAL 4 is considerably more than the lower EALs.

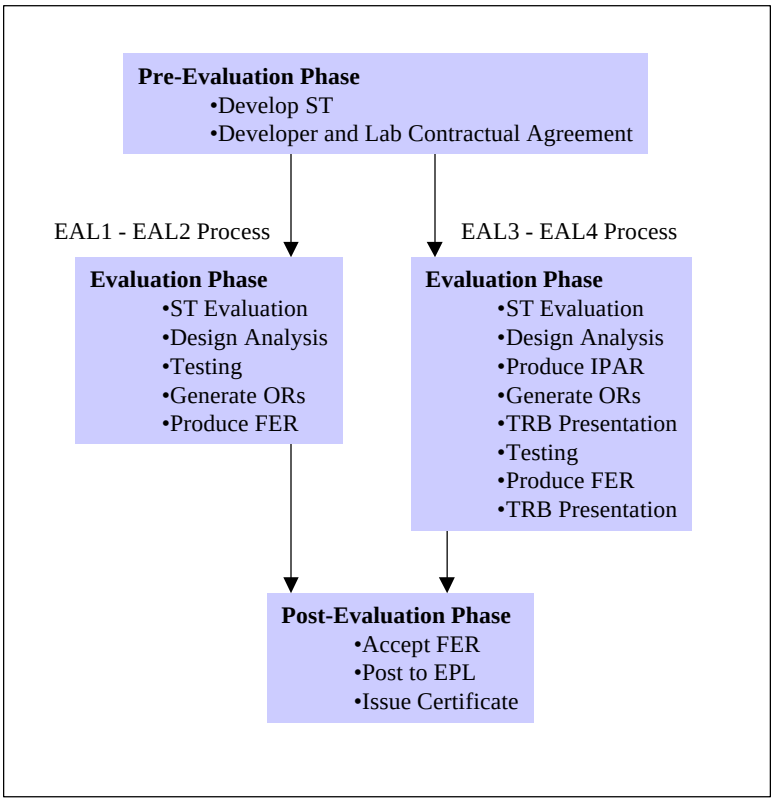

Figure 2 TTAP Evaluation Processes

Figure 3 presents the evaluation phases under the NIAP Scheme. The Developer should note that under the NIAP Scheme, an evaluation must be formally accepted by the Validation Body before proceeding. Formal acceptance requires review of the ST, evaluation work plan and evaluation schedule by the Validation Body. The Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme for IT Security - Organization, Management and Concept of Operations* [5] does not differentiate between the evaluation process for each EAL but rather describes the number, type, and intensity of technical oversight activities as depending on:

- the assurance requirements that appear in the ST;
- the complexity of the TOE; and

- the experience of the lab in evaluating IT products in the identified technology area.

The Scheme Publication #3, *Common Criteria Evaluation and Validation Scheme for IT Security, Technical Oversight and Validation Procedures* provides the specific details of technical oversight.[8]

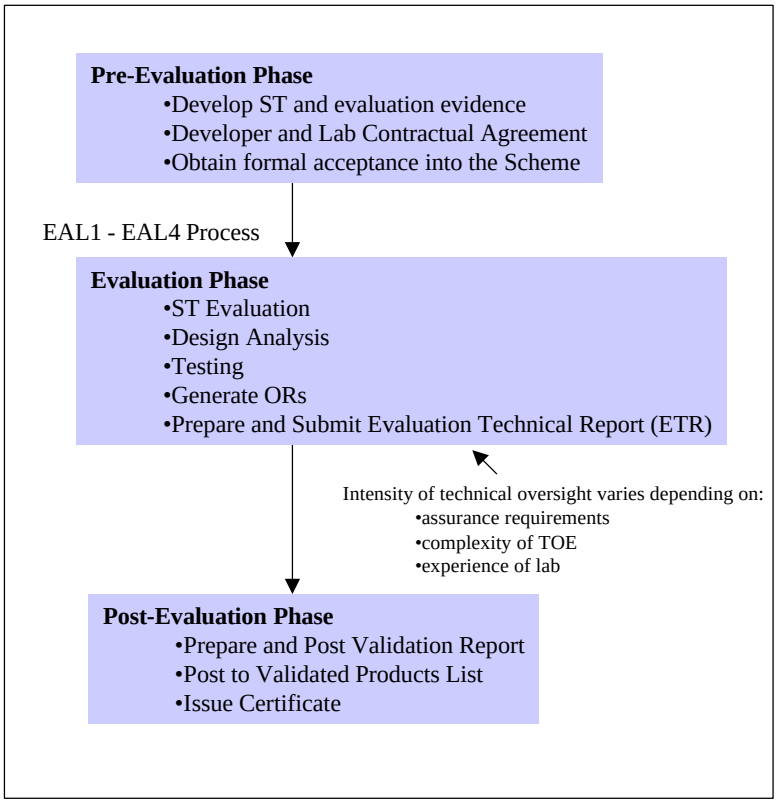

Figure 3 NIAP Scheme Evaluation Process

Regardless of what evaluation process is followed, the Developer must understand the level of commitment they are making when they enter into an evaluation. At a minimum, the Developer will incur the cost and commit resources to:

- train the evaluators about the evaluated version of the product;
- create and update evaluation deliverables (see Understand Evaluation Deliverables below);
- respond to technical questions about the product;
- participate in meetings with the lab (i.e., evaluation team) and Validation Body;
- provide a product for testing purposes; and
- manage the contract with the lab.

For a successful evaluation, it has been our experience that the lab and Developer should communicate regularly. This is especially true for the lower EAL evaluations because the schedule is short such that quick reaction and response is critical to avoid schedule slips. The Developer should also keep in mind that although the lab is an independent party to assess the product, the Developer has contractual control over the lab to honor the agreed upon evaluation work plan.

---

[8] As of this writing of the paper, Scheme Publication #3 has not been published.

Understand the Evaluation Deliverables

Critical to any evaluation are the availability of evaluation evidence and the definition of the TOE in its evaluated configuration. The Developer must be clear in the ST about what is being evaluated as the TOE and what is the evaluated configuration. The resulting certificate applies only to the specific version and release of the IT product in its evaluated configuration. Table 2 identifies the evaluation deliverables that are required for a CC evaluation.[9] It is important for the Developer to understand that these deliverables must be in a state that can be used for an evaluation. They must be complete, current with respect to the product, correct, and at a minimum contain the information as stated by the appropriate *Content and Presentation of Evidence Elements* requirements. The Developer is encouraged to reuse evidence used under another evaluation scheme (i.e., ITSEC) if appropriate.

Table 2 CC Evaluation Deliverables

Evaluation Deliverable	EAL1	EAL2	EAL3	EAL4
Configuration Management Plan			•	+
Configuration Management Documentation	•	+	+	+
Configuration Management Acceptance Plan				•
Delivery Procedures		•	•	+
Installation, Generation, and Startup Procedures	•	•	•	•
Functional Specification	•	•	•	+
High-Level Design		•	+	•
Implementation Representation				•
Low-Level Design				•
Correspondence Analysis[10]	•	+	•	+
TOE Security Policy Model				•
Administrator Guidance[11]	•	•	+	•
User Guidance[12]	•	•	+	•
Analysis of Guidance Documentation				•
Development Security Documentation			•	•
Life-cycle Definition Documentation				•
Development Tools Documentation				•
Test Coverage Analysis		•	+	•

[9] A bullet denotes the deliverable is required for the EAL. If no change in content is required for the next higher EAL then a bullet is repeated. If a change in content occurs in the next higher EAL, a plus sign is used.

[10] Although the ADV_RCR.1 requirement for correspondence analysis is the same for EAL 1 – EAL 4, the adjacent pair of TOE Security Functions representations changes at EAL 2 and at EAL 4.

[11] Although the AGD_ADM.1 requirement for administrator guidance is the same for EAL 1 – EAL 4, the AVA_MSU.1 requirement levies additional content requirements for guidance documentation at EAL 3.

[12] Although the AGD_USR.1 requirement for user guidance is the same for EAL 1 – EAL 4, the AVA_MSU.1 requirement levies additional content requirements for guidance documentation at EAL 3.

Evaluation Deliverable	EAL1	EAL2	EAL3	EAL4
Test Depth Analysis			•	•
Test Documentation[13]		•	+	•
TOE Test Suite[14]		•	+	•
TOE for testing	•	•	•	•
Strength of Function Analysis		•	•	•
Vulnerability Analysis		•	•	+

The Developer should note that not all the evidence needed is something they would normally already have. Although EAL 1 and EAL 2 assurance requirements are inline with best commercial practices for product development thus allowing the Developer to use existing documentation as evidence, there are some requirements in the CC that require the Developer to develop new documents or addendum. The Developer should pay close attention to the installation, generation, and startup procedures, users guidance, administrator guidance, and test documentation requirements. These requirements ask for specific descriptions relating to security and the TOE in the evaluated configuration. Also, it has been our experience that Developers tend to underestimate the test documentation requirements. It is strongly recommended that the Developer understand the documentation requirements before finalizing any evaluation schedule. Lastly, the Developer must understand that the evaluation team will find problems in the evidence and that it is the Developer's responsibility to address these problems. The Developer should not underestimate the number of iterations that may occur for resolution. The corrections must be reflected in the final set of evaluation evidence so the evaluation team can confirm the evidence as satisfying the requirements.

Choose a Laboratory

A major decision a Developer is faced with is choosing a laboratory to conduct the evaluation. Picking a laboratory is critical for a Developer because the timeliness and cost of the evaluation effort hinges on the competency, experience, and work ethic of the evaluation team members. How does a Developer pick a laboratory? It is the Developer's best interest to choose a laboratory that is authorized to conduct CC evaluations under a scheme that falls under the auspices of the Mutual Recognition Arrangement. In the U.S., certificates produced under TTAP and the future NIAP Common Criteria Evaluation and Validation Scheme for IT Security are mutually recognized by the countries who signed the Mutual Recognition Arrangement.[15]

It is recommended that a Developer takes advantage of the competitive market and solicit proposals from the various authorized laboratories to perform the evaluation. Unless the Developer has first hand experience and knowledge of a lab's abilities, it is prudent for the Developer to investigate what the various labs are offering. The Developer should issue a Request For Proposal (RFP) to their lab(s) of choice. It has been our experience that some Developers have solicited all the labs while others have pre-picked two or three based on reputation and popularity. The RFP should be specific in the information

[13] Although the ATE_FUN.1 requirement for test documentation is the same for EAL 2 – EAL 4, the quantity of information the must be provided varies in accordance with the test coverage analysis and test depth analysis.

[14] Although the ATE_IND.2 requirement for sample testing is the same for EAL 2 – EAL 4, the test suites provided by the developer is dependent on the test documentation.

[15] It should be noted that the Developer is not restricted to picking a lab in the U.S. because of the Mutual Recognition Arrangement does have the option to solicit labs in other countries. This paper's focus is Common Criteria evaluations in the U.S. The authors do not mean to exclude other options for the Developer.

requested so the lab can precisely answer the RFP and the Developer is able to compare proposals based on the same criteria. Typical items to request in an RFP include a proposed work plan, schedule, estimated cost, resumes, experience with the product technology, and evaluation experience. The work plan and schedule are important items for they are required when applying for evaluation under the NIAP scheme.

When reviewing proposals, it is reasonable to first compare them. It has been our experience that cost and schedule are driving factors when choosing a laboratory. However, the Developer should not be surprised if the schedules and costs are not comparable. Again, CC evaluations are new and for the most part the labs are making educated guesses as to what it will take to perform the evaluation. There currently aren't any historical data to rely on to determine which bid is reasonable. Areas that a Developer should consider when examining proposals are the location and reputation of the laboratory, past performance, presentation of the proposal, and the lab's experience with the product and/or technology. Ultimately, with these considerations, the Developer can be confident that an informed decision was made.

Maintaining the Certificate

Once the evaluation is over and a certificate is issued for the product, the Developer's next worry is how to maintain the certificate for future versions or releases of the product. The CC describes an assurance maintenance paradigm and defines a set of assurance requirements called the Maintenance of assurance class (AMA). Because the analysis of AMA requirements isn't a formal program under TTAP, Developers have chosen to address the maintenance of their certificate by re-evaluation. Essentially, the laboratory would have to evaluate the product as though it was a new evaluation. It would behoove the Developer to choose the same laboratory that conducted the original evaluation such that evaluator findings could be reused, as appropriate, and training minimized. A Certificate Maintenance Program (CMP) is defined under the NIAP Scheme and requires the Developer to produce plans and procedures for assurance maintenance and to appoint a Developer Security Analyst (DSA). The Developer must request entry into the CMP at the start of the initial evaluation and the ST must include assurance maintenance requirements. The assurance maintenance plans and procedures are evaluated by the laboratory and approved by the Validation Body as part of the initial TOE evaluation. Once the initial evaluation is completed, the DSA ensures that the TOE is maintained according to the assurance maintenance plans and procedures. Periodically, the laboratory will independently check the developer's compliance to the plans and procedures. The laboratory will write a Certificate Maintenance Report (CMR) which is reviewed by the Validation Body and if appropriate the Validation Body will issue a new certificate for the product reflecting the new version or release numbers. At some point, depending on the number of changes or significance of change(s), a re-evaluation of the TOE will occur. Specifics about the CMP are described in Scheme Publication #6, *Common Criteria Evaluation and Validation Scheme for IT Security - Certificate Maintenance Program*.[16]

Conclusions

It is obvious that the consumer receives many benefits by purchasing an evaluated product. In addition, the Developer will also profit from having their product evaluated to the requirements of the CC. These benefits are highlighted as follows:

[16] As of this writing of the paper, Scheme Publication #6 has not been published

- The CC is an International Standard. Successful CC evaluations are recognized worldwide with Canada, France, the UK, Germany, and the U.S. signing an arrangement of mutual recognition. The product will need to undergo only one evaluation to be recognized by all these nations.[17]
- Consumers are aware that evaluated products have received an independent third party endorsement of the their security functionality. An authorized lab contracted by the Developer conducts the evaluation.
- CC evaluations are conducted in comparatively less time than TCSEC evaluations. The Developer is better able to provide an evaluated version of the product that coincides close to its release cycle.
- A successful CC evaluation will permit entry and acceptability in specialized markets such as US government and private industries.
- The evaluation process will help to refine and improve the product's security functionality.
- Evaluation of the product demonstrates the Developer's commitment to security. The Developer's claims are verified.

With these benefits in mind, the Developer should also understand that CC evaluations in the US are happening *now*. Although these evaluations are performed under a transition program (TTAP), the establishment of NIAP Scheme is imminent. Certificates received under TTAP will be recognized under the NIAP Scheme. The Developer should visit the following TTAP and NIAP web sites to keep current on the latest progress with CC evaluations, available PPs, and evaluated products: www.radium.ncsc.mil/tpep and www.niap.nist.gov.

Acknowledgements

The authors would like to thank H Patrick Dunn for suggestions and comments.

References

[1] *Common Criteria for Information Technology Security Evaluation Criteria*, Version 2.0, May 1998.

[2] *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

[3] *Information Technology Security Evaluation Criteria*, Version 1.2, 28 June 1991

[4] *Common Evaluation Methodology for Information Technology Security*, Version 0.6, dated January 1999

[5] *Common Criteria Evaluation and Validation Scheme for Information Technology Security - Organization, Management and Concept of Operations*, Scheme Publication #1, Version 2.0, dated May 1999.

[6] *Common Criteria, An Introduction* Pamphlet, Version 2.0

[17] It is planned that other nations will sign the mutual recognition arrangement.