atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: 512-615-7300
Fax: 512-615-7301
www.atsec.com

Efficient Common Criteria Evaluations

Written by Stephan Mueller, atsec information security corporation: April 10th, 2006

In March 2006, the United States Government Accountability Office (GAO) issued an assessment regarding Common Criteria certifications and the work performed by the US oversight institution NIAP called "Information Assurance – National Partnership Offers Benefits, but Faces Considerable Challenges"[1].

The current article prepared by atsec information security corporation, an accredited laboratory experienced in the evaluation of large software components, explains how these challenges can be mitigated and which are, in fact, already addressed in current Common Criteria evaluations performed by atsec. We conclude that all four challenges outlined by the GAO can be addressed within the current setup of the Common Criteria methodology and the CC Evaluation and Validation Scheme implemented by NIAP. Many of the issues set forth by the GAO report can be mitigated by adopting innovative approaches that enhance the efficiency of the evaluation process. atsec has already demonstrated that such an efficient work style is possible to cover a large portion of the challenges addressed by the GAO report.

Before analyzing the challenges outlined by the GAO report, we want to stress that the GAO findings do not constitute a negative report expressing that the Common Criteria evaluation methodology has not been proven a success. The GAO document explains that the Common Criteria evaluation system involves several participants: the vendor of an IT product; the evaluation laboratory evaluating the developer's product; the validation body, which in the US is CCEVS, overseeing the evaluation laboratory's work; and the governmental agency or consumer relying on the CCEVS certificate that is issued after a successful evaluation.

Based on this scheme, the GAO report identifies benefits "to using the process for use in national security systems". The identified benefits include:

- Appreciation of an independent evaluation and testing of an IT product
- International recognition of the evaluation results, allowing a broader product selection
- Assessment of the functionality of an IT product, including identification and remediation of flaws
- Improvements in the vendor's development process, helping to improve the overall quality of the current and future products.

These findings are supported by the results of a survey of 24 federal agencies performed for the GAO report.

In addition to the explanations of the benefits of the "NIAP Evaluation Process", the GAO report also provides suggestions for improvements. The report identifies the following challenges that are to be used as a basis for the improvement of the whole evaluation process:

- NIAP-evaluated products do not always meet agencies' needs, which limit agencies' acquisition and use of these products.
- A lack of vendor awareness of the NIAP evaluation process impacts the timely completion of the evaluation and validation of products.
- A reduction in the number of validators available to certify products could contribute to delays in validating products for agency use; and

[1] The document is labeled with GAO-06-392 and can be downloaded at http://www.gao.gov/new.items/d06392.pdf.

- A lack of performance measures and difficulty in documenting the effectiveness of the NIAP process makes it difficult to demonstrate the program's usefulness or improvements made to products' security features and functions or improvements to vendors' development processes.

The remainder of this article analyzes each of the GAO's identified challenges and provides either suggested solutions or explains already practiced methods of addressing these challenges.

NIAP-evaluated products do not always meet agencies' needs, which limit agencies' acquisition and use of these products.

Ideally, evaluated products are useful; that is, after the evaluation process culminates in issuing a certificate, an agency acquires that product because it matches a need. The likelihood that evaluated products will fill agencies' needs can be increased using several available strategies:

- Developing useful Protection Profiles
- Using a "staged" evaluation strategy, so that initial evaluation of a product at a lower evaluation level builds a good platform for later evaluation at a higher level
- Pursuing ongoing communication between agencies, vendors, evaluation labs, and NIAP, so that emerging agency requirements on mature product lines are clearly understood by all parties in the evaluation process
- Conducting development, Common Criteria consulting, and Common Criteria evaluation efforts in parallel, so that certification of new products is timely (atsec example: Red Hat Linux evaluation project)

Each of these strategies is discussed further below.

Protection Profiles

The Common Criteria methodology provides a general mechanism for how users or consumers of IT products should inform vendors about a product's security functional requirements. Consumers can develop Protection Profiles (PPs), which define a minimum set of security functionality that must be implemented if a product is to be successfully evaluated based on such a Protection Profile. During acquisition, consumers just need to check whether a product has been successfully evaluated using the consumer's required Protection Profile. The use of Protection Profiles is the standard approach for instructing vendors about functional requirements provided by the Common Criteria framework, whereas other means of communication may be employed between customers and vendors.

A number of Protection Profiles have been developed in recent years by US government agencies (only a part of the PPs have been developed by NSA) which can be used in Common Criteria evaluations. Examples of such Protection Profiles for operating systems are the Controlled Access Protection Profile (CAPP)[2] or the Labeled Security Protection Profile (LSPP)[3], which are frequently used in evaluations of operating systems. Such Protection Profiles may also be developed by commercial vendors.

[2] This Protection Profile is the successor to the orange book level C2 - http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.html.

[3] This Protection Profile is the successor to the orange book level B1 - http://niap.nist.gov/cc-scheme/pp/PP_LSPP_V1.b.html.

Staged evaluation strategy

As the development of such a Protection Profile requires considerable effort, this process may not be suitable for communicating the extension of the scope of an evaluation, such as a request to include a particular feature of a product in the evaluation assessment. In these evaluations, we observe a strategy by vendors in the development of the scope of evaluations pursued. Initial evaluations of products are performed to demonstrate that the vendor is able to provide the necessary assurance about the functionality of the product as well as the development process. These initial evaluations are characterized by a narrow functionality and complexity that adheres closely to the requirements set forth by a Protection Profile. This allows the initial evaluation to pass with a reasonable effort and duration.

Clear communication of emerging functionality

For newer evaluations of maturing product lines, we identified that vendors are now adding new functionality claims to be evaluated for a particular product. Based on discussions with the vendors, these newly added functions are now subject to scrutiny by the evaluator due to their usage at governmental agencies. We conclude that vendors are communicating with agencies about what kind of functionality is being used and should therefore be considered in an evaluation. Examples of products with a much broader functional scope than that required by the claimed protection profiles are Windows, AIX, and z/OS. Such additional functionality in recent evaluation projects of operating systems covers Kerberos, LDAP authentication, NFSv4, IPv6, IPSEC and others. Furthermore, previous operating system evaluations usually claimed conformance with CAPP, but recently vendors required the inclusion of additional functionality claimed by LSPP. The effort of vendors to meet the security functional requirements of their customer base is obvious in the public development effort for adding Mandatory Access Control, Role Based Access Control, and enhanced auditing capabilities to Linux. The public project encourages hardware vendors, including IBM and HP, software vendors, such as Red Hat, with its upcoming Red Hat Enterprise Linux version 5, and other Open Source developers as well as potential customers, such as NSA to support the joint development of needed functionality. Additionally, atsec provides consultancy support for all parties to ensure that all requirements of the Protection Profiles are met.

Note that the mechanisms offered by Common Criteria with respect to Protection Profiles, informal discussion, and development rounds are neither to be enforced nor initiated by CCEVS. This effort has to be addressed by the vendor and the consumer.

Parallel development/consulting/evaluation efforts

Evaluation laboratories may also support this effort, providing guidance that all functional requirements are implemented. In order for an evaluation laboratory to provide such consulting services, while complying with the impartiality requirements for evaluators, these commercial laboratories may create a consulting team that is completely separate from the evaluation team.

atsec Example: Red Hat Enterprise Linux evaluation project

Considering the example of the ongoing Linux development effort, the consultation of an evaluation laboratory during product development allows the vendor to prepare for a fast, efficient evaluation. In addition to the consulting services, the evaluation effort for the upcoming Red Hat Enterprise Linux product is already initiated in parallel with the development and considers the newly developed functionality. The goal is for the evaluation to finish quickly, within a month after the product becomes generally available.

This effort now can and should be supported via NIAP oversight, ensuring that the CCEVS validation processes support these vendor strategies. As atsec delivers interim evaluation reports to CCEVS, these reports can be used for early review by the validator as atsec ensures that the differences between these interim reports and the final evaluation conclusions are kept to a minimum.

There are even successful examples of evaluations being performed by atsec in parallel with the vendor's development at the German certification body, the Bundesamt für Sicherheit in der Informationstechnik (BSI), the German counterpart of US NIAP. The certificate for the AIX operating system version 5.2 at EAL4[4] has been awarded within four weeks of the announcement of general availability. A similar effort has been conducted for the evaluation of the operating system SUSE Linux Enterprise (SLES) version 9, service pack 2 on SGI hardware[5].

A lack of vendor awareness of the NIAP evaluation process impacts the timely completion of the evaluation and validation of products.

As previously outlined, the communication of functional requirements from consumers to vendors can be achieved by developing a Protection Profile, or by adopting a product line evaluation strategy. Such effort, however, requires an in-depth knowledge about how Common Criteria is to be applied.

atsec's opinion is that the current approach of the CCEVS does lack appropriate training of the participants of the Common Criteria evaluation process. Nevertheless, in the US, there are commercial offers for such training that when applied appropriately can support the evaluation process.

In Europe, Common Criteria evaluations are standard for the product type smart cards. In this industry appropriate specialist know-how has to be transferred to vendors and consumers of smart card products. One method of providing this information is through the training offered by the German BSI to evaluators, vendors, and consumers to ensure that all involved parties "speak the same language". Similarly, this knowledge transfer could also be achieved by CCEVS training, at least to the governmental agencies, in how Common Criteria is to be applied and how requirements can be communicated to vendors.

One additional measure of how to ensure that agencies and vendors work together efficiently may be the involvement of consultancy services by qualified personnel with significant Common Criteria experience. As previously discussed, this consultancy should cover guidance for all participants to ensure that security functional requirements are appropriately communicated and correctly implemented.

A reduction in the number of validators available to certify products could contribute to delays in validating products for agency use

The mutual recognition arrangement (CCRA) covering Common Criteria evaluation up to an evaluation level of EAL4 allows vendors to have products evaluated at certification bodies in member states of the arrangement. Because of the flexibility offered by the CCRA, if the urgency to complete a specific product evaluation doesn't match with available NIAP CCEVS resources, a vendor could consider pursuing certification through the expanded pool of validators available via international certification bodies who are part of the CCRA.

Within the realms of the current CCEVS scheme for Common Criteria evaluations, the certification of a product can be achieved within a reasonable time frame for both the consumer and the agency when performing an evaluation that proceeds in parallel with the development. An example of current

[4] The certification ID is BSI-DSZ-CC-0194, the certification report can be found at http://www.bsi.bund.de/zertifiz/zert/reporte/0304a.pdf.

[5] The certification ID is BSI-DSZ-CC-0292, the certification report can be found at http://www.bsi.bund.de/zertifiz/zert/reporte/0292a.pdf.

efforts is given above with the Linux evaluation. A key to the success of such an approach is for the evaluation labs to consistently deliver complete, high-quality evaluation work and results, so that the validator can limit the scope of his or her activity to the intended validation role.

A lack of performance measures and difficulty in documenting the effectiveness of the NIAP process makes it difficult to demonstrate the program's usefulness or improvements made to products' security features and functions or improvements to vendors' development processes

The Common Criteria and the NIAP validation scheme allow the assessment of a product to require that certain functional claims are met by a vendor. The evaluation assessment performed by accredited laboratories allows the identification of the effectiveness of the evaluation. Numerous implementation issues, design changes, as well as guidance enhancements are usually stimulated by the evaluation work for an evaluation.

However, in the realms of Common Criteria methodology and the CCEVS, the measurement of effectiveness of a single evaluation is hard to demonstrate. The whole process of evaluation and validation contributes to the improvement of IT products, but this improvement is as difficult to show as for other, non-CC validation efforts. For example, the annual vehicle inspection required in the US is designed to also ensure that vehicle safety mechanisms are functioning effectively. However, the measure of effectiveness of those inspections does not necessarily correlate well with highway accident statistics published the US National Transportation Safety Board. In like manner, providing measures for the effectiveness of Common Criteria evaluations is similarly hard to achieve. We prepared and held a presentation for a colloquium given at the Swiss Federal Institute of Technology in Zurich which provides details about possible measurements of the effectiveness of a Common Criteria evaluation[6].

Additional aspects to be addressed

In addition to the challenges outlined in the GAO report, we consider the currently missing assurance maintenance measures as an issue to be addressed by NIAP in order to allow Common Criteria to gain greater acceptance.

A Common Criteria certificate today only applies to the exact version of the IT product that was subject to evaluation. Updates, such as bug fixes and even enhancements, always require a reevaluation of the product. As a conventional reevaluation requires greater resources on the part of the vendor, validator and evaluator, a timely completion of such a reevaluation is hard to achieve.

However, if an assurance maintenance plan can be set up and agreed upon by the vendor, the validator, and the evaluator, an efficient and rapid assessment of bug fixes and small functional changes can be performed to ensure that these patches are also covered by the Common Criteria certificate. NIAP needs to provide guidance on how such a reevaluation process can be integrated into the NIAP scheme, making the most effective use of a security-aware development process, an efficient assessment of the security implications of changes by the evaluation lab, and fast publication of the successful reevaluation on the NIAP web site.

---

[6] ZISC Information Security Colloquium SS 2005; publications to be retrieved at http://www.zisc.ethz.ch/events/infseccolloquium2005 - the referenced presentation can be retrieved at http://www.zisc.ethz.ch/events/ISC2005Slides/KurthCertifications.pdf

Another aspect neglected so far is an alignment of the CC evaluation with system certification processes within the US government. The use of evaluated products does not guarantee security when those products are integrated into a system. The US government has defined processes for system certification and those processes on the one hand need to be supported by evaluations and on the other hand should provide guidance to the vendors about the environment their products are intended to operate in and the security functions that are expected to be subject to an evaluation. An appropriate alignment with projects like FISMA can ensure that system integrators as well as end users can get the best benefit from a Common Criteria evaluation. A joint effort between NIAP and other US government initiatives to increase the security of critical IT systems should be started to better define the place of Common Criteria evaluations within the overall effort for more secure information systems.

Conclusion

The GAO report outlines the strengths and weaknesses of the Common Criteria methodology with respect to their practical implementation with the CCEVS.

The identified strengths include:

- Appreciation of an independent evaluation and testing of an IT product
- International recognition of the evaluation results, allowing a broader product selection
- Assessment of the functionality of an IT product, including identification and remediation of flaws
- Improvements in the vendor's development process, helping to improve the overall quality of the current and future products.

In addition to enumerating the benefits of the NIAP evaluation process, the GAO report also identifies the following weaknesses in the current implementation of the process:

- NIAP-evaluated products do not always meet agencies' needs, which limit agencies' acquisition and use of these products.
- A lack of vendor awareness of the NIAP evaluation process impacts the timely completion of the evaluation and validation of products.
- A reduction in the number of validators available to certify products could contribute to delays in validating products for agency use; and
- A lack of performance measures and difficulty in documenting the effectiveness of the NIAP process makes it difficult to demonstrate the program's usefulness or improvements made to products' security features and functions or improvements to vendors' development processes.

The weaknesses identified by the GAO are valid and present challenges that Common Criteria participants must address. Most of the identified weaknesses can be mitigated within the current bounds of the Common Criteria and the CCEVS by adopting innovative approaches that enhance the efficiency of the evaluation process. Suggestions for process improvements include facilitating development of useful Protection Profiles; ensuring that all parties understand both agency needs and emerging technologies; staging evaluations such that initial evaluations at lower EALs build a good platform for later more rigorous evaluations; conducting development, consulting, and evaluation efforts in parallel whenever possible; offering expanded Common Criteria training opportunities; and requiring high-quality evaluation work and results from the evaluation labs so that validators' time is well spent.

Several additional issues are not specifically discussed in the GAO report but should be addressed by the Common Criteria community when considering improvements to the evaluation process. Assurance maintenance measures to create an avenue for quick reevaluation of updates to certified

products must be developed. In addition, alignment of CC evaluation with system certification processes within the US government will enhance the value of both programs.

As the evaluation role is largely performed by commercial evaluation laboratories, it makes sense for NIAP to address potential solutions for these issues jointly with all accredited laboratories. The examples provided throughout this article may be useful to all evaluation participants in achieving a process that is efficient and acceptable.