NSA/CSS Commercial Solutions Center (NCSC)

# Common Criteria Reforms

Better Security Products through Increased Cooperation with Industry

*Chris Salter*
*1/10/2011*

This paper is an explanation of the criteria being used by NIAP to help champion a new direction for the Common Criteria Community.

The Common Criteria for Information Technology Security Evaluation is a framework for testing products against security claims. The Common Criteria Recognition Agreement (CCRA) is an understanding among more than 20 countries to recognize commercial evaluations overseen by 13 of its members.

In theory, countries that recognize Common Criteria evaluations should have considerable clout for convincing vendors to make security improvements to products. In practice, these countries have not cooperated sufficiently to agree upon requirements and many participants do not require the evaluations. The current trend is for countries to create their own testing regimens.

In some cases, these competing evaluation schemes will be used to protect indigenous industries, and, more disconcertingly, as an opportunity to force vendors to disclose sensitive information. Costly and time consuming evaluations by individual countries will create trade barriers for international sales of IT products and disclosures of sensitive information will put intellectual property of companies at risk while making it easier for its adversaries to find flaws in products.

No individual country, though, has the resources to write requirements for all technologies that matter or has the clout with vendors to result in significant security improvements in products. The reforms to Common Criteria outlined in this paper are intended to make Common Criteria into the brand that represents “due diligence” for the security testing of an IT product. The intent is to create a larger market for Common Criteria evaluated products that would provide greater incentive for vendors to participate and greater clout for governments to foster significant improvements in security. The proposed changes in governance would give a larger role to industry and are intended to ensure fairness and to bring into play the significant security expertise that industry has to offer.

## CRITERIA FOR SUCCESS

The reforms are intended to convince enterprises to request that IT products be Common Criteria evaluated. But causing more sectors of society to insist on these evaluations should not be the only criterion for success.

The first two criteria are straight forward. Government has a responsibility to ensure that evaluations are:

- **Consistently applied to competitors**
- **Produce comparable and meaningful results**

To be fair to smaller vendors, no requirement should drive up costs and time to market unless it can be justified for what it accomplishes for security and unless the requirement is applied with the same diligence to a competitor.

Government benefits if there is a wide selection of products and thus if industry has a large incentive to participate. Thus it is important for that government to ensure that evaluations are

- **As inexpensive and as quick as possible**
- **Accepted in the widest possible market**

The innovations in information technology are outpacing the ability to deploy the new capabilities safely. It is important to ensure that vendors are trying to differentiate themselves with better security features and are not prevented from participating by unnecessarily expensive or time consuming evaluations. Participation in the

Common Criteria community and evaluations can be more easily justified if the costs can be amortized over larger markets.

Vendors have concerns about the loss of their intellectual property (IP), especially when detailed design documents and source code are required to be disclosed as evidence for an evaluation. Access to code and other low level documents make it easier for attackers to find flaws. For most technologies, however, evaluators cannot find all flaws and are unlikely to find the same vulnerabilities as an attacker. Government should be prudent then about requirements to disclose sensitive information to 3rd parties and the procedures that are used to handle sensitive information.

Government should thus strive to ensure that evaluations:

- **Only require vendors to disclose information that can be used effectively by any evaluator**

Most of all, of course, government has a responsibility to ensure evaluations are effective.

## EFFECTIVENESS

Ultimately, enterprises will require product certifications because they address how adversaries exploit products.

Adversaries seek flaws in how a product is:

- **designed**
- **developed**
- **deployed**
- **handled during its life cycle (supply chain)**

Common Criteria currently focuses on design features and their implementations. High level threats are used to justify specific features such as an audit system or role based access control that differentiates between user and administrative privileges. The evaluator seeks to confirm that features are correctly implemented and that the product's design is sound[1].

Common Criteria is weaker at addressing the other three types of flaws. To address development mistakes such as buffer overflows, some evaluations do include vulnerability discovery and testing; for deployment, the vendor is required to provide a configuration guide for the correct administration of the product; and for life cycle threats, there is a nominal verification of the configuration control of the product.

The Common Criteria model thus allows all four aspects of product security to be addressed. The question then is how to address all components more effectively and in a manner that meets our criteria and convinces purchasers of the value of the evaluations.

## THREE STEPS

Three steps must be taken to convince governments and enterprises to require Common Criteria evaluations.

---

[1] Eric Bidstrup from Microsoft wrote about how Common Criteria needs to better address these types of flaws in his blog posting "Common Criteria and answering the question 'Is it Safe.'

The first step toward rebuilding the Common Criteria brand is to get the criteria themselves out of the way. The public documents that are currently produced are too high level and too encumbered by Common Criteria jargon. The fix is to write documents that are more specific and more understandable to those responsible for IT security in their organizations.

The second step is to write requirements for a technology that includes the vendors that build the products. Currently, each country is allowed to write a Protection Profile for a technology that describes threats to be addressed and the features expected from a product to mitigate the threats. The U.S., several of the other countries and vendors have started to write "Standard" Protection Profiles for technologies that:

- **Provide a complete set of understandable threats**
- **Have a negotiated set of functional features that is as specific as possible**

The intention is that any security professional should be able to readily understand what types of problems are being addressed and should be confident that all aspects of product security are being considered. The security functional features should all be justified in simple prose against the threats being addressed.

The third step is the hardest and most crucial. A tailored evaluation methodology has to be created for each technology area.

Twice, the Common Criteria community has tried to instill greater confidence in the effectiveness of its evaluations by changing the criteria themselves. What is needed, though, is an acknowledgement that no single set of criteria can be used to produce comparable and effective evaluations for a wide range of technologies.

Currently, no evaluator activities are specified in a Protection Profile. Instead, evaluation activities have been defined for all technologies by the Common Criteria Evaluation Methodology (CEM) supporting document recognized as part of the mutual recognition agreement. This is a general set of evaluation activities that make no reference to a specific technology.

The primary reason that Common Criteria has not achieved its potential is that none of the original countries was willing to commit to the expense in time, money, and personnel to tailor an evaluation methodology to a technology. The pressure was to put Common Criteria in place to evaluate all Information Assurance (IA) and IA related technologies as quickly as possible.

## IT TAKES A COMMUNITY

The Common Criteria Community must evolve into a standards body that has a separate track for each technology. Each technology community would develop its own threat model, functional requirements, and evaluation methodology. (This is what the European smart card community accomplished with the European Union under a more narrow mutual recognition agreement). A major benefit of this approach is that the confusion about the meaning of Evaluated Assurance Levels (EALs), which is merely a measure of evaluation effort but not of security soundness, will disappear when all products are evaluated to the same extent and in the same fashion against a methodology tailored to a technology.

To be successful, each technology track must be open to all vendors, to all countries in the mutual recognition agreement, to all critical sectors such as finance, health, and transportation, and to the evaluators in the labs. The tailored criteria must be created in the same fashion as a protocol or standard created by groups such as the Internet Engineering Task Force.

## A SOUND COURSE

The recommended reforms address all government responsibilities and meet the criteria for success.

The Common Criteria will be consistently applied and produce comparable results because the evaluation methodology will be tailored specifically to a technology. The evaluation methodology can specify the evidence that the developer should produce while building a product, the actions that should be taken by an evaluator while assessing the product, and, perhaps most importantly, can establish criteria for validators to apply consistently to developer evidence and evaluator testing.

An additional benefit of writing requirements before a product is built is that evaluations can more likely depend upon evidence naturally produced during a product's development. The delay and costs of having a third party generate evidence after a product is created could be eliminated.

Vendors will have an equal voice in deciding when it is necessary to put at risk intellectual property such as source code. All such disclosures will have to be justified against a threat model and what is being accomplished for security.

The market for Common Criteria evaluations will expand when the believability of the effectiveness of an evaluation increases. If all critical sectors and most vendors participate in a standards effort to establish clearly what constitutes "due diligence," this provides a baseline for future improvements and an inducement for more enterprises to buy evaluated products.

## CONCLUSION

Commercial information technology products are the foundation for the security of our information infrastructure that has no logical or physical borders. Commercial IT is rapidly becoming the security command and control for our physical infrastructure. It is past time for governments and industry to make a more significant investment in an international standards effort for security requirements and testing that is warranted by our increasing reliance upon information technology. It is time to transform the Common Criteria for Information Technology Security Evaluation framework into a standards body for fostering the security needed by society for IT products.