Global Information Assurance Certification Paper

The Common Criteria for Information Technology Security Evaluation – In with the new and out with the old

Jeff Knight
Dec 9, 2000

Introduction

Every day we take for granted the security and reliability of household products. Your wife uses a hairdryer right over the bathroom sink, and isn't electrocuted. A consumer notices the UL label on products and assumes it means the product is safe, but what protection or advice is offered when an IT Professional buys security products?

Are you currently using ICSA Labs and TruSecure, ITSEC or how about the Common Criteria Project (CC) as a means to verify product qualify? These groups offer insight as to how and even why the security products used day to day in your enterprise may be trusted(1,2,3).

This paper focuses on the Common Criteria Project, how it works and what it means to the INFOSEC security product user and buyer. This is a high level introduction, with further reading referenced below.

What is the Common Criteria (CC) Project?

The CC is an international initiative by the following organizations: SCSSI (France), NLNCSA (Netherlands), CSE (Canada), BSI (Germany), NIST (USA), NSA (USA) and CESG (United Kingdom) to align the existing US, Canadian and European criteria, and to develop new criteria for evaluation of IT security products. This effort has developed into an International Standard (ISO 15408) - CC v2.0.

The great idea here is that CC will be used an a Common Evaluation Methodology and Scheme to allow independent laboratories to evaluate Targets of Evaluations (TOEs)– security products, that can lead to certified approval and registered certification of the product. This evaluation will be recognized across all seven organizations through a Mutual Recognition Agreement (MRA).

A Security Target (ST) is a container of security objectives and requirements specified in the TOE. The ST may claim conformance to one or more Protection Profiles (PPs). A Protection Profile is a reusable grouping of security requirements defined for common security objectives. For instance, there are PPs for databases, firewalls and even backward compatibility to the TCSEC standards. (7)

The last main piece of the CC pie is the Evaluation Assurance Level (EAL). Assurance levels define a common scale for evaluation of the PPs and STs. There are seven

assurance levels, ranging from EAL1 – functionally tested to EAL7 – formally verified design and tested.

The following chart compares EALs, TCSEC and ITSEC levels.(9)

CC	US TCSEC	Euro ITSEC
	D: Minimal Protection	E0
EAL 1		
EAL 2	C1: Discretionary Security	E1
EAL 3	C2: Controlled Access	E2
EAL 4	B1: Labeled Security	E3
EAL 5	B2: Structured Protection	E4
EAL 6	B3: Security Domains	E5
EAL 7	A1: Verified Design	E6

You should start using the CC

Many infosec professionals believe the good old "tried and true" TCSEC – Orange book - is all they need. That would be fine except that direction from the US Government has explained that the Trusted Product Evaluation Program (TPEP) and the Trust Technology Assessment Program (TPAP) will no longer accept new evaluations based upon TCSEC starting 1 February 1999. The CC must used, and by the end of year 2001, all formerly evaluated products against TCSEC will become obsolete or must be reevaluated by the CC process.(8)

Questions asked while purchasing security products lead directly to the CC and the need for certification

Let's take a firewall for example, Marcus Ranum offers these questions - please notice the red highlighted sections: (5)

- **Security:**
  *What are the security design principles of your firewall?
  *Why do you think it is secure?
  *What kind of 3rd party expert review has it been subjected to?
- **Corporate credentials:**
  *How long have you been selling this firewall?
  *What is the size of your installed base?
  *Do you have reference accounts that we can contact?
- **Support and engineering:**
  *How many full-time support engineers do you have?
  *What hours does your support operate?
  *How much does technical support/maintenance cost?
  *What is your patch/upgrade policy?
  *Does the product include any type of warranty for the hardware or software?

- **Documentation:**
  *Request a copy of the documentation for review
  *What kind of audit reports does the firewall generate? Request a copy of an audit report for review.
- **Operational:**
  *Does the firewall include hardware or is it just software?
  *What kind of network interfaces does the firewall support? (Will you need token ring to Ethernet routers, for example?)
  *What is the management interface of the firewall like?
  *Is the firewall remotely manageable? How is remote management secured?

As you can see, buying a security product forces an understanding of risk and evaluation of the underlying product. Who do you trust? Why is the product secure? In the CC case, a buyer can look at the evaluation and examine the Protection Profiles and Security Target information for the Target of Evaluation – product itself. This provides rationale if the boss asks "why did you pick X over Y?. (6)

Look at a sample vendor's firewall site, in this case Checkpoint Firewall 1. The CC certification is right up on top. You will also notice the ITSEC and ICSA logos for ratings as well, but the prediction is, down the road there will be more and more CC ratings and less and less of the others. Time will tell. (4)

Summary

The bad news is TCSEC is out of date and ready for replacement. The good news is there is a replacement - the Common Criteria for Information Technology Security Evaluation, and it is recognized internationally.

Commercial vendors have started using the CC, it has become an ISO standard, and the government is backing it totally. What are you waiting for?

Reference:

Internet

(1) The ICSA Labs home page.
http://www.icsa.net/html/labs/

(2) The UK ITSEC home page.
http://www.itsec.gov.uk/

(3) Common Criteria Information page
http://csrc.nist.gov/cc/info/infolist.htm

(4) Checkpoint Firewall-1 Certification explanations
http://www.checkpoint.com/products/certifications/

(5) Ranum, Marcus. "How to Pick an Internet Firewall." October, 1998.
http://www.icsa.net/html/communities/firewalls/buyers_guide/app_b.shtml (18 Sep. 2000)

(6) Checkpoint Firewall-1 CC Certificate – NIAP validated product list
http://niap.nist.gov/cc-scheme/CCentries/TTAP-CC-0006.html

Books

(7) *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general Model*, May 1998. Version 2.0, CCIB-98-026

(8) K. Minihan. *Advisory Memorandum on the Transition from the Trusted Computer System Evaluation Criteria to the International Common Criteria for Information Technology Security Evaluation.* Mar 99, NSTISSAM COMPUSEC/1-99.

(9) *Common Criteria, An Introduction,* Pamphlet by Syntegra