Common Criteria and Packages

In the last couple of years I've heard various discussions, about evaluation assurance levels, or EALs in the abbreviated language of Common Criteria.

Some comments are sadly misguided: I've had people call me on several occasions to say things like: "I'd like to get an EAL please" and "EAL 4 is better than EAL 2". I've heard people claim that "EAL 1 is useless" and that "EAL 7 is the holy grail" and even "My product is better than yours because it has a higher EAL".

So, one common theme that often strikes me when I hear these kind of discussions is that the ordinary security assurance consumer has no clue what an EAL actually is. Here's an attempt to explain it, and perhaps allow us to consider the statement "Let's not have an EAL at all" in an informed way.

Common Criteria Packages

The Common Criteria allows for two kinds of special construct to support consumer groups, or technical communities in expressing their requirements for security assurance. These are called "Protection Profiles" (PPs) and "Packages". When we discuss EALs it is the "Package" construct on which we focus our attention.

A package as defined in the Common Criteria is a **named** set of security requirements. It can be made up of either a set of functional security requirements, or of a set of security assurance requirements. Note that packages containing both security functional and assurance requirements are not allowed. A package can be defined by anyone with the goal of communicating a set requirements that are useful, effective and the package should also be reusable.

Note that it is not compulsary to use any packages when undergoing evaluation.

The Common Criteria standard goes so far as to some Packages of security assurance requirements itself (in part 3). One set of Packages are the familiar set of seven evaluation assurance level (EAL) packages. Another set of Packages are the composed assurance packages (CAP) , named CAP-A, CAP-B and CAP-C, which are to be applied when composing several already-evaluated components in order to provide security assurance about the whole..

The other construct allowed in the Common Criteria standard to communicate the needs of the various communities is the more familiar Protection Profile. A protection Profile describes the general requirements for a technology type and is usually used as a template for the Security Target documents used to define the specific target of an evaluation. A Protection Profile may reference packages, but not vice versa. A Security Target document may contain statements that claim conformance to Protection Profiles and/or Packages.

About the Evaluation Assurance Level (EAL) Packages

Each EAL package, from "evaluation assurance level 1 - 7", gives a set of security assurance requirements drawing from the assurance classes of development, guidance documents, life-cycle support, testing, vulnerability assessment and security target evaluation.

Section 8.1 of Common Criteria 3.1 Rev 3 gives an complete overview of the evaluation assurance levels: The EAL packages are each described using a unique name, the objectives of the package are given, application notes are provided, and the chosen assurance

components for that EAL are given. Note that the producers of the packages ensured that any dependencies were addressed within the package.

Although according to part 1 of the standard using the EAL packages is not mandatory, it is important to consider that the EAL packages have been defined within part 3 of the Common Criteria standard itself since it's inception. So the EAL packages have become de-facto constructs in the language of Common Criteria. They have become institutionalised in the procurement language and regulations of many of the 26 certificate consuming governments and many user communities, procurement agencies and others that rely on them to describe the level of assurance that is needed for their own security case.

Not only are EAL packages often cited as a procurement requirement by assurance consumers. They have also been built into the language of internationally agreed mutual recognition arrangements such as the Common Criteria Recognition Arrangement (CCRA), and the MRA known as SOGIS, the Senior Officials Group – Information Systems Security which is a body of the European Commission. These are build on a common understanding of the assurance drawn from the use of such an agreed and specified package.

Evaluation assurance level 1 (EAL1) - functionally tested

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation**.**

Evaluation assurance level 2 (EAL2) - structurally tested

EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.

Evaluation assurance level 3 (EAL3) - methodically tested and checked

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed

EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

Evaluation assurance level 5 (EAL5) - semiformally designed and tested

EAL5 is applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested

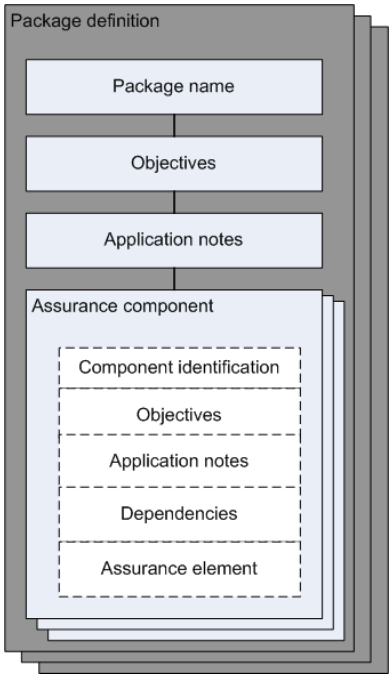
EAL6 is applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.

Evaluation assurance level 7 (EAL7) - formally verified design and tested

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

The definition of new packages

It is also perfectly legitimate for anyone to define a definition of a package of assurance or functional requirements. If, for example one of the proposed Common Criteria technical communities were to agree such a definition, then these packages themselves could be re-used in several PPs. As stated earlier these packages could contain either assurance OR for functional security requirements. It has already been suggested that a set of packages for supply chain assurance be formulated in this way. If compatibility to the CCRA or SOGIS is desired then these new packages would need to take care that an existing EAL package was not disrupted by their use.



The figure to the left is derived from Common Criteria part 3, illustrates the contents of a Package

It is worth mentioning one technique of package development that some people have found useful. This is the technique of specifying that “refinement” be the only operation allowed for assurance components which allows the Package developer to express technology specific details of assurance components relating to technology specific assurance details, while remaining compatible with the CCRA. An example of this technique was the expression of assurance aspects of FIPS 140-2, that was used in some Hardware Security Module Protection Profiles.

Food for thought

Not specifying an EAL package for an evaluation is legitimate in terms of the Common Criteria standard, but by not doing so several political implications are created.

1. The CCRA and SOGIS agreement will still be applicable to the mutual recognition of certificates that do not directly claim an EAL, provided that all the assurance components in the package claimed are contained in either EAL 1,2, 3, or 4 or belong to the ALC_FLR family.

2. According to the CCRA document additional assurance levels may be agreed at any time and ratified by the signatories. This would open the possibility of defining new assurance levels that would be recognised. This process has already been performed since the components for flaw remediation (ALC FLR) was agreed to be accepted by the various signatories.

3. The security assurance consumers will need to pay a very close analysis of the assurance case that they specify vs the security assurance offered by the certified product that they wish to procure or use. Since without reference to the familiar EALs the security assurance objectives of a Protection Profile or Security target document will need to be ellucidated in order to determine if they match the needed assurance case.

4. The CC community (CCMB/CCDB) do not have a formal mechanism for registering packages and their definitions. This is something that may be needed if technical communities decide to use the package construct more widely.

Problems have been cited as associated with EAL package conformance claims. The psychological effect of numeric "grades" has been misinterpreted by non-security

professionals and badly misused in some marketing efforts, after all "an EAL 7 must offer the best security", which of course is not true. Like all things CC, the focus is on providing assurance, i.e. confidence that the security claims are true. The great thing about this is that an assurance consumer can match the assurance given by a particular evaluation to the needed assurance case, which is usually closely linked to their own organizational security objectives and policies. There is no need to pay for the provision of assurance that is not needed.

Some claim that the EALs specify assurance requirements that are not needed. This may be true, but the rationale for this statement must to be explained since it is the assurance consumer that should make this call and that ultimately relies on the assurance provided in maintaining their security stance. Developers, of course also need to understand the requirements levied on them through the specification of various security assurance requirements.

Packages are a very powerful tool. However, outside of the Evaluation Assurance Level packages they have not been used very often. That they are powerful is evidenced by the success of EALs. Technical communities considering working on Protection Profile developments should also familiarize themselves with the packages concept, since these too can be just as useful as a Protection Profile. This is especially true when considering security requirements that may be used across several technology types or that is intended for use in several Protection Profiles, especially when using the refinement technique described above.