Foundations of Computer Security

Lecture 80: Common Criteria Evaluations

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Assurance Levels

Evaluation under the Common Criteria targets a specified level of rigor. The vendor provides assurance that the corresponding rigor was applied during development and test.

EAL1: *Functionally Tested*

EAL2: *Structurally Tested*

EAL3: *Methodologically Tested and Checked*

EAL4: *Methodologically Designed, Tested and Reviewed*

EAL5: *Semiformally Designed and Tested*

EAL6: *Semiformally Verified Design and Tested*

EAL7: *Formally Verified Design and Tested*

Evaluation Levels

Level	Requirements	Functional Specification	High-level Design	Low-level Design	Implementation
EAL1	Informal	Informal	Informal	Informal	Informal
EAL2	Informal	Informal	Informal	Informal	Informal
EAL3	Informal	Informal	Informal	Informal	Informal
EAL4	Informal	Informal	Informal	Informal	Informal
EAL5	Formal	Semiformal	Semiformal	Informal	Informal
EAL6	Formal	Semiformal	Semiformal	Semiformal	Informal
EAL7	Formal	Formal	Formal	Semiformal	Informal

The CC Certificate

Issuing a CC certification means that the government of the country where the evaluation is performed believes the evaluation was conducted properly.

Indicates a good faith effort to ensure the product meets the claims of the vendor. Does not assure absolute correctness or suitability to particular requirements. Does not preclude vendor "over-marketing."

Later versions may require re-testing.

Mutual Recognition

The governments of 26 countries now formally recognize the Common Criteria.

Have mutual recognition of evaluations performed by labs in each other's countries, up to EAL4.

Testing Labs

Product vendors cannot self-certify; evaluation tests must be performed by an independent organization accredited to perform CC testing. NIST is responsible for managing this process in the U.S.

Evaluations are performed (for a fee) by commercial laboratories that are certified by NIST (National Institute of Standards and Technology).

Independent labs test up to EAL4. Currently 10 labs in the U.S., with one (atsec) in Austin.

Testing costs are driven by a relatively small market, complexity and need for a skilled staff.

- EAL2 costs \$100K to \$170K and takes four to six months
- EAL4 costs \$300K to \$750K and takes one to two years.

Evaluation above EAL4

A product to be tested at EAL5/EAL6/EAL7 must have been designed using formal (mathematical) methods.

- Can't reverse engineer the model from the code.
- Components should be kept small and independent.

Extensive documentation is required.

In the U.S., only NSA performs testing for EAL5 and higher. A U.S. agency would not accept a certification for EAL5 or above issued by another country.

Lessons

- Evaluation Assurance Levels (1–7) define the care with which the product was developed and the rigor of the evaluation process.
- Certification by a country means that the evaluation was carried out carefully and in good faith, not that the product is suitable or secure.
- Evaluations are performed by independent labs for a fee. The labs are licensed by the national testing authority.