Evaluation of Security

Prof. Dr. Eşref ADALI

www. Adalı.net

Scope of Evaluation

- Target
- Organizational framework
- Purpose
- Structure of Criteria
- Method
- Cost and Benefit

Target of Evaluation

- In the goal of evaluation there are products and IT systems.
- Hardware and software are the products of IT system.
- Operating system and application software are software products.
- Some of the software are COST product that we can buy.
- Some of the software are in house product that we have to develop them.

- Product has to meet security requirements
- System has to meet the specific requirements of a given application

- The Trusted Computer System Evaluation Criteria; (TCSEC), DoD 1985
- Information Technology Security Evaluation Criteria ; (ITSEC), EU 1991
- Federal Criteria; (ABD NIST and NSA, 1992)

Purpose of Evaluation

There are three purpose of evaluation

- **Evaluation** : Assesses whether a product has the security properties claimed for it.
- **Certification** : Assesses suitability of a product or system for a given application.
- **Accreditation** : Decide to use a certain IT system.

Method of Evaluation

The evaluation method must find the security problems. Different evaluations of the same system or product must generate the same result. There are two different evaluation methods may be used:

- Product oriented method : In this method, product or system is examined and tested. This method is good to find problems.
- Process oriented method : In this method evaluation is done on documentation and product development process. This method is easy and cheaper than product oriented method.

Organizational Framework

Evaluation may variate according to organization framework. For example evaluation in public and private organization is different.

- Public organization : Evaluation process are slow in public organization and be difficult to retain qualified staff for long time.
- Private organization : Evaluation process may be done by organization staff or a certificaiton agency.
  - In private organization, we have to make sure that there is no relationship between evaluation sponsor, product producer and evaluation facilities.
  - The other important issue is that customer pressure does not influence evaluation results .

Note : Interpretation of criteria may change over the time and differ between evaluators

Structure of Evaluation Criteria

- The structure of evaluation Criteria are:
- Functionality : Functionality is the security features.
- Effectiveness : Effectiveness are the appropriate use of mechanisms.
- Assurance : Assurance is the integrity of analysis

- Orange book consider all three aspects at the same time.
- ITSEC consider all three aspects independently.

Cost and Benefits

Cost

Evaluation of IT system has two kind of cost:

- **Direct costs** : The fees is directly paid for evaluation process.
- **Indirect costs** : Indirect costs consists of employee time, training cost, impact cost on development process.

Benefit

If you have evaluate your IT system, you may get some contracts of government or other company

The Orange Book

Developed in 1967 by DoD for national purpose but today is used in more general. It provides:

- For users to assess the degree of trust in computer security system.
- Guidance for manufacturers of computer security system.
- A basis for specifying security requirements when acquiring a computer security system

Evaluation Classes

- Security Policy
- Marking of objects
- Identification of subjects
- Accountability
- Assurance
- Documentation
- Continuous Protection

Security Classes (TCSEC)

Level	Classe-1	Classe-2	Classe-3
A Level : Verified Protection	A1		
B Level : Mandatory Protection (based on labels)	B1	B2	B3
C Level : Discretionary Protection (‘need to know’)	C1	C2	
D Level : Minimal Protection			

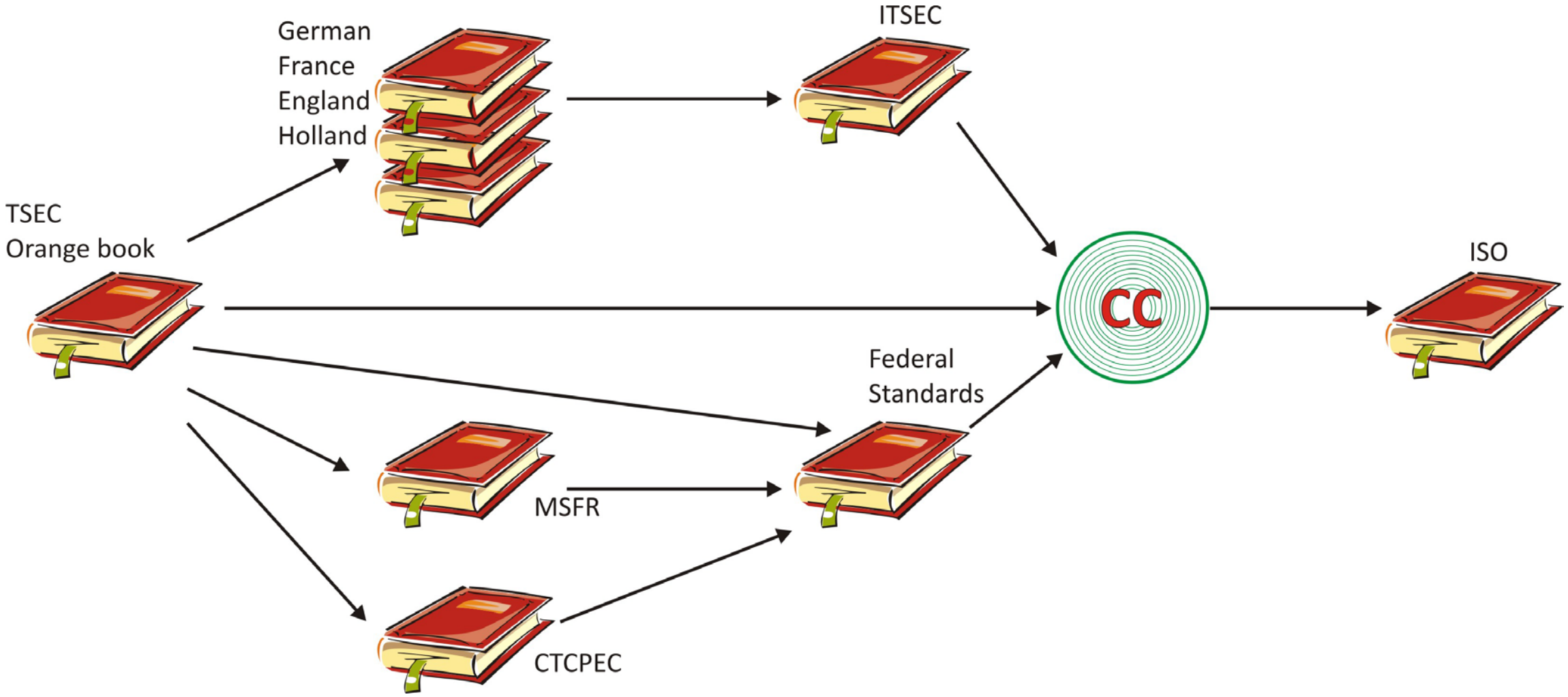
Europa

- Four EU member country (Germany, France, Holland and England) develop Information Technology Security Evaluation Criteria, (ITSEC)

The main components of ITSEC are:

- Confidentiality
- Integrity
- Accessibility

Common Criteria



Comparision of TCSEC, ITSEC and Common Criteria