

ECMA

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

STANDARD ECMA - 205

Commercially oriented functionality class for security evaluation (COFC)

December 1993

Free copies of this document are available from ECMA,
European Computer Manufacturers Association,
114 Rue du Rhône - CH-1204 Geneva (Switzerland)

Phone: +41 22 735 36 34 Fax: +41 22 786 52 31
X.400: C=ch, A=arcom, P=ecma, O=genevanet,
OU1=ecma, S=helpdesk
Internet: helpdesk@ecma.ch

ECMA

EUROPEAN COMPUTER MANUFACTURERS ASSOCIATION

STANDARD ECMA - 205

Commercially oriented functionality class for security evaluation (COFC)

December 1993

Brief History

In September 1990 the European Commission announced the "Harmonized IT Security Evaluation Criteria" ITSEC. The governments of France, Germany, Great Britain and the Netherlands had agreed on a common set of criteria for IT security evaluations. The European Commission proposed these criteria for usage within the European Community.

The ITSEC deviated substantially from the US TCSEC, (Trusted Computer System Evaluation Criteria) commonly known as Orange Book, the de-facto standard since 1983.

This created a problem for all world-wide operating computer manufacturers who were faced with two problems:

- to which set of criteria they should develop their products, and
- if a product was developed to one set of criteria, would a customer in a country outside the influence of this set accept the product and its evaluation.

Users of IT products were confused because they did not know, which set of criteria would meet their requirements.

The European Computer Manufacturers Association, ECMA, was alerted by its members, mostly world-wide operating companies. The ECMA General Assembly therefore decided already in December 1990 to establish an ad hoc group on Security. This group started its work in March 1991. Later in 1991 the group became ECMA/TC36 and then TC36/TG1.

The group decided to address the problem twofold:

- First, to write an ECMA Technical Report which positions security evaluations in the context of secure information processing in order to highlight the fact that an evaluated product or system can only guarantee security, when the total system, its environment and its operation are secure.
- Second, to develop an ECMA Standard for a functionality class which defines a minimum set of requirements for commercial application. This class was called "Commercially Oriented Functionality Class" or COFC. It distinguishes itself from the Orange Book and respective ITSEC functionalities, which are more tuned towards military and government requirements for confidentiality of classified information. Assurance criteria, as addressed on the Orange Book and ITSEC, have not been taken into account.

Both, the Technical Report and the Standard are intended to be a contribution to the ongoing harmonisation process. They highlight commercial requirements, which call for an appropriate evaluation process, ranging from vendor self-testing to accredited third party testing, and a minimal set of functional requirements, which satisfy commercial needs.

This ECMA Standard has been adopted by the ECMA General Assembly of December 1993.

Copyright European Association for Standardizing Information and Communication S

Table of contents

1	Scope	1
2	Conformance	2
3	References	2
4	Definitions	2
4.1	Terms defined in this document	2
4.1.1	Access right	2
4.1.2	Administration	2
4.1.3	Customer-specifiable	2
4.1.4	Identification	2
4.1.5	User identifier	2
4.2	Terms defined in other documents	3
5	Acronyms	3
6	Specification of security enforcing functions	3
6.1	Identification and Authentication	3
6.1.1	Unique Identification and Authentication	3
6.1.2	Identification and Authentication prior to all other interactions	3
6.1.3	Associate information to users	3
6.1.4	Logon message	3
6.1.5	Number of logon trials	3
6.1.6	Expiration of unused user identifiers	4
6.1.7	Disable users temporarily	4
6.1.8	User status information	4
6.1.9	Authentication information protection	4
6.1.10	Authentication information independence	4
6.1.11	Authentication information aging	4
6.2	Access Control	4
6.2.1	Authenticated user identification	4
6.2.2	Individual user	4
6.2.3	User groups	4
6.2.4	Objects	4
6.2.5	Types of access rights	5
6.2.6	Default access rights	5
6.2.7	Precedence of access rights	5
6.2.8	Date of modification	5
6.2.9	Verification of rights	5
6.2.10	Application controlled access rights	5
6.3	Accountability and audit	5

6.3.1	Associate actions and users	5
6.3.2	Logging	5
6.3.4	Copy audit trails	6
6.3.5	Alarm if unable to record	6
6.3.6	Select users	6
6.3.7	Dynamic control	7
6.4	Object Reuse	7
6.5	Accuracy	7
6.5.1	TOE software integrity	7
6.5.2	Data integrity	7
6.5.3	Security parameters status report	7
6.6	Reliability of service	7
6.6.1	Recovery	7
6.6.2	Data backup	7
7	Password specific requirements	7
7.1	User-changeable password	7
7.2	Password aging	7
7.3	Password expiration notification	7
7.4	Password reuse	7
7.5	Password complexity	8
7.6	Password logging	8
7.7	Default passwords	8
Annex A (informative)	Access control model	9
Annex B (informative)	Terms defined in other documents	11