Extending a Security Evaluation Standard (the ITSEC) to Dependability

Alan Hawes
Admiral Management Services Limited
Camberley, England

1. Introduction

1.1 Purpose of this Paper

This paper reports on some work which was performed on the Eagle Project to look at the ways in which an existing security evaluation standard could be extended to address safety issues. The Eagle Project was project number S2114 in the European Commission’s INFOSEC’93 programme of research.

The findings of the project are of interest to the safety community, because if these extensions are incorporated into security evaluation practice, a well established third party evaluation scheme, based on internationally agreed standards, will become available to developers of safety-critical systems.

Any discussion which bridges two fields - in this case safety and security - will inevitably hit difficulties of terminology, which will hinder understanding of the underlying concepts. While every attempt has been made to overcome this problem, the reader is asked to make allowances for any remaining ambiguities when assessing the proposals made in this paper.

1.2 Background to the Eagle Project

The Eagle Project was set up by the Commission of the European Community (CEC) during the two year period of trial use of the Information Technology Security Evaluation Criteria (ITSEC) Standard, as part of a number of initiatives to build on the experience of ITSEC in practical use. The standard was being applied in a number of community countries, and work was needed to coordinate the results of that experience in some recommendations for improvements to be made in the next version.

The ITSEC lays down an internationally agreed set of criteria to be used by evaluators when assessing the security characteristics of systems or products which
include IT components. The standard formed the basis of security evaluation and certification schemes in Germany and the UK, and it was anticipated that its use would spread to other countries.

At this time, a companion standard the Information Technology Security Evaluation Manual (ITSEM) was being produced, and it had provided some clarification and interpretation of the ITSEC, which was being used differently by evaluators in different Evaluation Facilities (ITSEFs). However it appeared that some areas, such as Re-evaluation needed additional work beyond the ITSEM's clarifications. In particular, there were some errors and ambiguities in the ITSEC which had not been addressed by the ITSEM.

The CEC INFOSEC'92 programme was at that stage underway, and had already produced some results which made recommendations for the extension of the ITSEC, particularly in the field of the interface to Accreditation.

When the project started, some initial work had been done by the Common Criteria Editorial Board (CCEB) to establish common evaluation criteria for use in Europe and North America. It was felt that the work done by the Eagle Project could provide input to that initiative, if the CCEB wished to establish criteria with a wider scope of applicability than the ITSEC.

1.3 Objectives of the Project

The Eagle Project was set up to meet two major objectives:

a. "The primary objective of this project is to recommend the way ahead for enhancing the ITSEC to cover the re-rating and re-evaluation of products and systems."

b. "A secondary objective is to make recommendations for widening the scope of the ITSEC to cover additional topics..." where these topics were to be defined by the project.

1.4 Scope of the Project

It was recognised that the project would need to be wide-ranging in scope, to address all the issues related to the potential extensions of ITSEC. The project was set up to collect data on the practical use of ITSEC, by having representatives from ITSEFs in a number of countries where evaluations are being performed.

The project was designed initially to seek input from a wide range of experts in the field with knowledge of ITSEC, in order to ensure that a wide range of views were considered and that consideration was given to the most important areas for