

# Toward a Medium-Robustness Separation Kernel Protection Profile

Rance J. DeLong  
Santa Clara University  
Santa Clara, CA  
rdelong@enr.scu.edu

Thuy D. Nguyen  
Naval Postgraduate School  
Monterey, CA  
tdnguyen@nps.edu

Cynthia E. Irvine  
Naval Postgraduate School  
Monterey, CA  
irvine@nps.edu

Timothy E. Levin  
Naval Postgraduate School  
Monterey, CA  
levin@nps.edu

## Abstract

*A protection profile for high-robustness separation kernels has recently been validated and several implementations are under development. However, medium-robustness separation kernel development efforts have no protection profile, although the US Government has published guidance for authoring such a profile.*

*As a step toward a protection profile, a set of security requirements for medium-robustness separation kernels is proposed. These requirements result from an informal, yet principled, approach. By bracketing the problem with appropriate reference points and elaborating a method for interpolating the requirements both a measure of uniformity and a basis for further discussion are achieved. Our reference points include the high robustness protection profile, the existing medium robustness consistency instruction, and our familiarity with the nuances of separation kernels.*

*This practitioner-oriented study is intended to advance the prevailing practices for commercial software development, which presently falls far short of the rigor needed for either high-robustness or medium-robustness systems. These requirements represent an incremental improvement in the pursuit of secure software — and is intended to be a step forward on the road to higher assurance.*

## 1 Introduction

The separation kernel [Rus81] has emerged as a promising foundation for the construction of highly secure systems [VBC<sup>+</sup>05]. In such applications a separation kernel must

exhibit high robustness in the face of attacks by resourceful adversaries against high-value resources under its control.

### Robustness

The Common Criteria addresses only functionality and assurance, not robustness. The U.S. Department of Defense defines three level of robustness: high, medium and basic. In this context robustness is “a characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly.” [DOD03] The robustness of a TOE represents the TOE’s ability to mitigate security threats in its operational environment. High robustness requires the security mechanisms to “provide the most stringent protection and rigorous security countermeasures” whereas medium robustness imposes requirements for “layering of additional safeguards above good commercial practices.” [DOD03] Best commercial practices are considered as basic robustness.

The Separation Kernel Protection Profile (SKPP) [SKP07] provides a set of security functional requirements (SFRs) and security assurance requirements (SARs) for separation kernels that will be employed in environments requiring high robustness. It admits implementations ranging from statically-configured partitioning kernels with coarse-grained information flow control enforcement through dynamically-configured kernels with a richer set of exported resources and corresponding fine-grained information flow control policy enforcement [LIN06].

Not every environment, however, requires such a high degree of robustness, since physical access constraints may guarantee a level of trustworthiness of individuals having access to the system. In such applications a medium-robustness separation kernel (MR SK) may suffice. Nevertheless, the prospect of using a common set of components and approaches to security engineering problems provides motivation for the existence of separation kernels that are largely feature-comparable to their high-robustness counterparts, but which are required to exhibit only medium robustness.

The U.S. Government has recognized a need for such a class of separation kernels, as evidenced by at least two developments: the publication by NSA of guidance for the application of both high- and medium-robustness separation kernels [NSA05b], and the determination by some DoD programs of the adequacy of a medium-robustness separation kernel for certain applications.

A proper protection profile (PP) for medium-robustness separation kernels would present both SFRs and SARs derived by a methodical analysis of the security environment and security objectives following the model of the Common Criteria [CC205].

This study proposes a set of requirements for medium-robustness separation kernels. Though informally derived, in contrast with the detailed analysis and justification required in a PP, these requirements are based on an interpolation of reliable sources informed by our familiarity with separation kernel requirements. We hope that providing this study can facilitate and provide consistency among ongoing development efforts, as well as offer a stepping stone to a PP. In addition, the separation kernel is one of many potential targets of evaluation that could exist in both high-robustness and medium-robustness implementations, hence a viable repeatable method for “requirements interpolation” could provide wider benefit.

## 2 Methodology

We wanted to study the security requirements for separation kernels suitable for deployment in environments requiring medium robustness, without taking on the considerable commitment of developing a protection profile.

We hypothesized that, given knowledge of the validated high-robustness SKPP, of medium-robustness consistency guidance, and of the nuances of separation kernels, then it would be possible to arrive systematically at a good approximation of the requirements for a medium-robustness separation kernel without incurring the expense of PP development.

The method should establish the reference points and the reasoning to be applied to allow interpolation of each requirement for medium robustness. Determining this *a pri-*

*ori* would reduce the variance of discretion applied among requirements. If a result appeared unsatisfactory, it could be analyzed to determine why, and then the method tuned and reapplied.

A strategic choice was to use the rationale provided in the SKPP as a key reference, because it is the most detailed written repository of knowledge concerning what makes a separation kernel unique. By applying rationale similar to that used in the SKPP, and making only the necessary changes while adjusting for the reduced assurance level, it is possible to have reasonable confidence that this informally derived set of requirements is a close approximation to that obtainable by a more rigorous analysis.

The methodology involved the following steps:

1. Collect relevant and documentation sources to *consider* for medium robustness guidance and, based on their applicability to this study, choose the final set to be *relied upon*.
2. Determine whether any security functional requirements in the SKPP could be dispensed with outright, or weakened, in a medium-robustness separation kernel.
3. Decide and finalize the functional requirements for a medium-robustness separation kernel, giving preference to functional interchangeability with the high-robustness separation kernel
4. Consider, in turn, each assurance family identified in the SKPP.
5. Identify an appropriate assurance component for each family based on the decision process detailed below in the Security Assurance Requirements section.

The functional and assurance requirements will be enumerated in later sections. The remainder of this section discusses the selection of sources used for the activity.

The assurance/robustness guidance documents identified for initial consideration were:

1. Separation Kernel Protection Profile (SKPP) [SKP07]
2. Common Criteria (CC) [CC205]
3. US Government Protection Profile for Multilevel Operating Systems in Environments Requiring Medium Robustness (MLOSPP)[MLO07]
4. IA Guidance for Systems Based on a Security Real-Time OS (IAG) [NSA05b]
5. Medium Robustness Consistency Instruction Manual (MR-CIM)[NSA05a]

The IAG recommends the use of “a Medium Robustness SRTOS<sup>1</sup> or a High Robustness SRTOS, depending on the scenario and a variety of factors.” Further, it states that a PP should comply with the MR-CIM and, as a starting point, use the security requirements from the SKPP and the assurance requirements from the MLOSPP.

A multilevel operating system is very different from a separation kernel. The MLOSPP describes a full-featured operating system with label-based security policy enforcement. The SKPP describes a minimal operating system that lacks not only label-based security but most of the services required of an OS meeting the MLOSPP. A separation kernel could be used as the foundation for implementing the features of a multilevel operating system, and must have at least the strength of function of any mechanism it is used to support. A version of the MLOSPP had been consulted as the SKPP was being developed, and its influence has already been distilled and filtered through the SKPP refinement process. Given the other more appropriate resources at our disposal we chose not to directly rely further upon the MLOSPP for the present exercise.

The IAG-provided guidance regarding medium-robustness separation kernel requirements is indirect: it merely cites other documents as sources for guidance. The documents cited are among those we considered, and the approach suggested by the IAG is very similar to the one described here, with the exception of the exclusion of the MLOSPP.

### 3 Security Functional Requirements

The SKPP describes a broad class of separation kernels. It is assumed that a medium-robustness separation kernel would be employed in a fashion architecturally similar to its high-robustness counterpart [NSA05b], though in a more sheltered environment. A medium-robustness separation kernel protection profile should reflect this assumption, as it engenders a commonality of components and approaches across the assurance spectrum, fostering cost savings and adaptability to changing environmental requirements.

For situations in which a SK security architecture is developed for an environment requiring medium robustness and then is later applied to an environment requiring high robustness, it would be advantageous if the medium-robustness separation kernel could be replaced by a high-robustness separation kernel with little or no architectural change. Therefore, it is proposed that a medium-robustness separation kernel have SFRs not substantially different from a high-robustness separation kernel, with the minor excep-

<sup>1</sup>The IAG defines an SRTOS as “a separation kernel-based Real-Time Operating System that has undergone an appropriate security evaluation.” In this study, such an operating system is generically referred to as a “separation kernel.”

tions noted in the following section. Thus, the greatest difference between a high-robustness separation kernel and a medium-robustness separation kernel would be the SARs.

### 4 Security Assurance Requirements

The security assurance requirements for evaluation of a medium-robustness separation kernel should be less demanding than those of the high-robustness SKPP. Table 1 summarizes the proposed SARs using SKPP nomenclature, providing information from the source documents for comparison and a reference to the discussion in the following sections. According to convention, component numbers not in parentheses (e.g., “3”) indicate an unmodified component from the Common Criteria catalog of SARs, while those in parentheses (e.g., “(3)”) indicate an explicit requirement. Numbering of explicit assurance components can be misleading. “(1)” is not necessarily a less demanding requirement than that represented by a “3,” or that represented by an explicit requirement “(2)” in another document. Some authors start numbering explicit requirements within a family starting at 1, while others use the number of the CC component most closely matching the explicit component. The “x’ ” and “x\* ” designations represent a decrease in the component leveling defined by the SKPP and MR CIM, respectively. The rationale for these changes is provided in the subsections associated with the corresponding families. The EAL 4 and EAL 6 columns represent the security assurance requirements in the standard package for each EAL given in Version 2.3 of the Common Criteria. The SKPP (HR) column gives the SARs from Version 1.03 of the SKPP. The MR CIM column gives the generic medium robustness requirements recommended by the Consistency Instruction Manual.

Though many of the MR SK requirements may correspond to those of MR CIM, a wholesale adoption of the MR CIM requirements is not appropriate for a separation kernel. Special considerations arise from the nature of a separation kernel TOE *qua* separation kernel, and these considerations apply generally to a MR SK as well as to one of high robustness, though the degree to which they may apply must be determined. These considerations played a role in defining the requirements presented here for a medium robustness separation kernel.

In some cases the medium-robustness requirement is derived in a similar manner to that of the corresponding SKPP requirement, though placed lower in the assurance hierarchy. As an example, consider the Functional Specification (ADV\_FSP) family. The CC EAL 6 package specifies component “3” (ADV\_FSP.3). The SKPP specifies ADV\_FSP.EXP.4, a tailored version of component “4,” while our medium-robustness requirement replaces the CC EAL 4 component “2” with a tailored version of component

**Table 1. Security Assurance Requirements**

Assurance Class	Assurance Family	EAL6 CCv2.3	SKPP (HR)	EAL4 CCv2.3	MR CIM	MR SK	MR SK Comment	See Section
Config Mgmt	ACM_AUT	2	2	1	1	1	MR CIM	§5.2
	ACM_CAP	5	5	4	4	4	MR CIM	
	ACM_SCP	3	3	2	2	2	MR CIM	
Delivery and Operation	ADO_DEL_EXP	2	(2)	2	2	(2)	NIST crypto	§5.3.1
	ADO_IGS	1	1	1	1	1		§5.3.2
Development	ADV_ARC_EXP		(1)			(1)	MR adjusted	§5.4.1
	ADV_CTD_EXP		(1)			(1)	SKPP	§5.4.2
	ADV_FSP_EXP	3	(4)	2	1	(3)	semiformal	§5.4.3
	ADV_HLD_EXP	4	(4)	2	1	(4)	SKPP	§5.4.4
	ADV_IMP_EXP	3	(3)	1	2	2	MR CIM	§5.4.5
	ADV_INI_EXP		(1)			(1)	SKPP	§5.4.6
	ADV_INT_EXP	2	(3)			(1)	MR CIM	§5.4.7
	ADV_LLD_EXP	2	(2)	1	(1)	(1)	MR CIM	§5.4.8
	ADV_LTD_EXP		(1)			(1)	SKPP	§5.4.9
	ADV_RCR_EXP	2	3	1	1	2	semiformal	§5.4.10
ADV_SPM_EXP	3	3	1	1	3	formal	§5.4.11	
Guidance Documents	AGD_ADM_EXP	1	(1)	1	1	(1)	SKPP	§5.5
	AGD_USR	1	1	1	1	1		
Life Cycle Support	ALC_DVS	2	2	1	1	1	MR CIM	§5.6
	ALC_FLR		3		2	2	MR CIM	
	ALC_LCD	2	2	1	1	1	MR CIM	
	ALC_TAT	3	3	1	1	2	+ impl stds	
Assur. Maint	AMA_AMP_EXP		(1)			(1)	SKPP	§5.7
	APT_PDF_EXP		(1)			(1)	mod'd SKPP	
Platform Assurance	APT_PSP_EXP		(1)			(1)	mod'd SKPP	§5.8.2
	APT_PCT_EXP		(1)			(1)	mod'd SKPP	§5.8.3
	APT_PST_EXP		(1)			(1)	mod'd SKPP	§5.8.4
	APT_PVA_EXP		(1)			(1)	mod'd SKPP	§5.8.5
	ATE_COV	3	3	2	2	2	MR CIM	§5.9
ATE_DPT	2	3	1	2	2	MR CIM		
ATE_FUN	2	2	1	1	1	MR CIM		
ATE_IND	2	3	2	2	2	MR CIM		
Vulnerability Assessment	AVA_CCA_EXP	2	(2)			(1*)	interpartition	§5.10.1
	AVA_MSU	3	3	2	2	2	MR CIM	§5.10.2
	AVA_SOF	1	1	1	1	1	MR CIM	§5.10.3
	AVA_VLA_EXP	4	(4)	2	3	3	MR CIM	§5.10.4

“3.” In a very few cases, the specified medium-robustness requirement is identical to that specified in the SKPP. Specific considerations influencing the determination of appropriate components are discussed in the following section.

## 5 Discussion of the Assurance Requirements

The following subsections describe the rationale used to derive the MR SK assurance requirements for each assurance class. In cases where explicit requirements from the SKPP are applicable to the MR SK, excerpts from the SKPP rationale for those explicit requirements are included.

### 5.1 A Note on Semiformal Style

It was necessary to define an appropriate guideline for “semiformal” for this study since the range of what can qualify as semiformal is very broad. *Informal* is defined as natural language, *formal* is defined as a restricted syntax language with formal semantics, and *semiformal* is anything in between. This would admit natural language with paragraph headings at one extreme and formal specification languages without a formal semantics at the other extreme.

To avoid ambiguity there needs to be a common language among the designer, the implementer, and the evaluator such that requirements can be interpreted the same by all. At a minimum, for semiformal notation we recommend a language with a defined syntax and a well-documented informal semantics that can support reasonably unambiguous compositional reasoning required for correspondence demonstration of evaluation evidences.

### 5.2 Configuration Management

The ACM class contains three families: CM Automation (AUT), CM Capabilities (CAP), and CM Scope (SCP). The requirements in this class are straightforward. The SKPP directly adopts the standard EAL 6 components for each family in the ACM class. The MR CIM similarly adopts the EAL 4 component. We follow EAL 4 and the MR CIM by requiring ACM\_AUT.1, ACM\_CAP.4 and ACM\_SCP.2.

### 5.3 Delivery and Operation

The critical nature of delivery is easily overlooked, but it provides a prime opportunity for subversion [Mye80]. In an environment where a separation kernel is used to isolate











