

A Note on High Robustness Requirements for Separation Kernels

Abstract:

The development of a protection profile for high-robustness separation kernels requires explicit modifications of several Common Criteria requirements as well as extrapolation from existing (e.g., medium assurance) guidance and decisions. The draft U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness (SKPP) is intended to be applicable to a class of products (the target of evaluation, or TOE) that includes, but is not limited to, real time and embedded systems. Other characteristics are that the products would not include a runtime user interface, would have a static runtime security configuration (with exceptions allowed for exigencies), would be capable of trusted recovery, and would export, but would not be required to maintain, audit records.

We describe the rationale for certain approaches and requirements that appear in the draft SKPP. Primary areas of focus are the information flow and dynamic configuration requirements. For highly robust security systems, the principle of least privilege (PoLP) is a significant factor that has not been explicitly addressed in the Common Criteria, to date. PoLP prescribes restrictions to actions of active entities including the internal modules and technical measures that comprise the TOE security functions, and the active subjects (e.g., application programs) in the TOE scope of control. In the SKPP, the restriction is that these entities must not have any more “privilege” (viz., access to resources) than is necessary to perform the actions for which they were designed. Exceptions to this requirement are allowed for certain degenerate designs.

A completely static separation kernel would maintain during runtime the time and space resource allocations and allowed interactions (i.e., information flows) with which it was initialized. Its design and implementation could be relatively simple and small, while providing a fundamental security service (viz., separation) upon which more complex systems could be constructed. However, in some scenarios (e.g., the failure of a peripheral device in a mission critical application), it may be desirable for the TOE to be able to change its security configuration. Thus, the SKPP allows the TOE to change resource allocations and allowed interactions (etc.) during runtime to another, pre-loaded, configuration.