

Compositional Assurance for IMA

John Rushby

Computer Science Laboratory
SRI International
Menlo Park CA 94025 USA

The IMA certification considerations issued as DO-297 and ED-124 are non-compositional much of the evaluation is performed on the fully assembled system and depends on testing more than analysis.

I will present an approach to compositional assurance being developed for the MILS security architecture. The assurance considerations in MILS and IMA are similar but not identical. I will attempt to distinguish where the analytical approach of MILS is effective and where the more empirical approach of IMA seems necessary.