File 20100509.1246: Notes for ACM workshop paper:

Title: Information Asymmetry in Cross Domain Accreditation

Abstract:

The theoretical difficulty of cross domain systems emerges from the fact that by definition they span at least one boundary between security domains controlled by different data owners. Consequently, new installations of certified solutions regularly encounter security testing criteria that represent the duplicated responsibility for residual risk of multiple data owners. Each data owner perceives a different set of risks A that would be desirable to mitigate, a set of risks B it is possible to mitigate, and their relative complement $A - B$, being the set of residual risks acceptable not to mitigate. Time and cost inefficiency in multilateral cross domain system accreditation to this point arises necessarily from asymmetry of knowledge, but there is room for a solution: the developer or installer of a cross domain system may know about extant risk mitigations that not all data owners are cleared for. If it were possible securely to establish amongst data owners a concord about the true extent of residual risk resulting from overlapping risk mitigations and testing, the unnecessary cost of duplicated effort could be greatly reduced. In support of this goal, a new tool, called nihil obstat, is being developed at the University of Oxford to present accreditation data in a common format.

References