Position Statement regarding the CC evaluation of Enterprise Security Management Products

Summary:

Given the imprecise definition of what constitutes an ESM product, it has proven infeasible to construct a meaningful PP or suite of PPs. The writing of a small set ESM PPs took an all-inclusive approach, which was appropriate given the vagueness of the security problem definition, resulted in PPs that are unsuitable for objective and repeatable evaluations. Therefore, at this time, we will not support or endorse any efforts to produce ESM cPPs.

Detail:

Enterprise Security Management (ESM) is not well defined, and consequently means different things to different people. To some it simply means a capability, such as centrally managing a corporation's audit or access control policies. To others it includes a set of products or components that are used to manage and enforce security policies. There are a number of products that claim to provide some form of ESM, which allows an organization to specify policies that are meaningful to that specific organization. These products provide a wealth of capabilities an organization may wish to employ, such as defining abstractions of objects they wish to control access, or allow for the specification of monitoring network traffic, or audit trails in a manner that is relevant to that organization, or control access to services provided by servers. Typically, these products are applications that run on one or more general purpose operating systems and define rules and abstractions that are transparent to the underlying platform. In some cases, the ESM product is installed into an operating system with full privileges, which, of course, introduces new attack surfaces.

Given the nebulous nature of products in the "ESM technology class" it has proven difficult to write meaningful Protection Profiles and the results of these efforts have been unsatisfying. The resulting PPs are written with open-ended (*assignments* to be filled in by the product developer) security functional requirements (SFRs) that can be satisfied by a wide range of products (even those that are not desirable) that make it near impossible for end-users to make meaningful product comparisons. Furthermore, when evaluating a product against these open-ended SFRs, it requires an evaluator to rely on their expertise and develop evaluation methods/techniques based on their individual experiences to assess the product's compliance to the SFRs in the PP. The result is a subjective evaluation that would not be repeatable if performed by a different evaluator. Another consequence is the result could be a product that provides little or no value, yet receives a CC certificate.

We believe there are products that are useful to an organization, such as an authentication server, an audit server, a firewall, etc., and they can be evaluated in a meaningful manner. While there appears to be a need for ESM functions or capabilities to effectively manage these products, at this time, it is our opinion that any assessments of this class of products is better suited to be performed by an organization that is deploying such products, and does not lend itself to an objective repeatable evaluation methodology.

Therefore, our position, at this time, is that constructing meaningful collaborative PPs for this class of products that is of value to our customers is impractical at this time, and we would not support or endorse such an effort.