

Position Statement regarding the CC evaluation of DBMS

Summary:

At this time, we see no value in a collaborative Protection Profile for DBMS security for Government use. Should an international Technical Community be formed for this topic, our position statement will state that this lacks relevance to Public Sector enterprise security needs.

Detail:

A Database Management System (DBMS) is a class of technology products providing an interface (user or programmatic) to an underlying structured database system. DBMSs can contain various controls to try and prevent or constrain certain interactions with the underlying database. Good practice for enterprise security recommends that DBMSs should be deployed as part of an n-tier security architecture.

As a direct consequence, the few security controls that a DBMS provides are difficult to analyse for effectiveness without the assessor having an understanding of how they are being integrated into a particular scenario. They cannot be looked at in isolation from the wider system and the defence-in-depth mechanisms which it collectively provides.

Given the primary route of attacking databases is not by defeating absent or weak DBMS security controls, we believe requiring vendors to undertake an evaluation process to assure these controls would not be a proportionate response.

We therefore concluded that the DBMS technology class is not currently amenable to the type of objective, and isolated, testing that CC can provide. We do not see development of standards to support such testing as being a priority at this time.