Position Statement regarding the CC evaluation of General Purpose Operating Systems

Summary:
A key point of the CCMC Vision statement is, “The general security level of general ICT COTS certified products needs to be raised without severely impacting price and timely availability of these products.” In the case of General Purpose Operating Systems, raising the general security level without severely impacting price and timely availability is not attainable under the monolithic evaluation approach used to date.

Given the complex nature of a General Purpose Operating System (GPOS), the wealth of features, and sheer number and complexity of the interfaces, we believe it is impractical to perform an evaluation using the CC as has been done in the past. Therefore, were an iTC to create a cPP that attempts to specify security functional and assurance requirements for a GPOS, our position is that such an evaluation would not be meaningful to our customers. We would therefore not endorse or support the creation of a cPP, nor recommend products evaluated against such a cPP.

Reasons why a GPOS cPP is not appropriate include:

- Inability to perform a cost-effective and comprehensive assessment of a GPOS in a reasonable timeframe
- Lack of objective evaluation activities

Detail:
General Purpose Operating Systems range from software products that run on a wide variety of commodity hardware platforms, to mainframes running on specialty built hardware. This class or technology type is intended to serve a multitude of uses and environments, including tablets, single-user workstations, servers, and mainframes. The notion of a “one size fits all” evaluation for Operating Systems has proven to be inefficient and does not improve the security of products.

**Lack of objective evaluation activities:** given the diversity of uses and environments, constructing a useful Protection Profile (PP) has proven to be a formidable task. The threat environment is very different if one is considering what security functional requirements (SFRs) make sense for a tablet vs. what is appropriate for a file server or a mainframe. Attempts to create a one size fits all PP requires that the SFRs contain assignments that are filled in by the GPOS developer, and this in turn makes it nearly impossible to ensure objective, repeatable evaluator activities can be consistently applied when conducting a Common Criteria (CC) evaluation.

GPOSs attempt to suit the needs of a wide range of users, resulting in exceptionally large and extremely complex products. The number and complexity of interfaces exported by these products is vast and complete testing of all of them is a daunting task. Interfaces include graphical user interfaces,
programmatic interfaces, command line interfaces, which may be accessible remotely and/or locally. While some interfaces are well-defined and documented, many others are not (e.g., they use shared memory to pass data, may not be advertised). Experience has shown that in order to evaluate a GPOS in a timely manner (years) and at a reasonable cost, a scoping effort is necessary to reduce the number of interfaces that are to be documented and tested. In other instances, rather than test all the interfaces a “gray-box” approach is taken to verify the correctness of the implementation. In order to perform this type of analysis, the evaluator must examine source code and have a detailed understanding of the product’s design. This subjective task relies heavily on the expertise of the evaluator.

**Inability to perform a cost-effective and comprehensive assessment of a GPOS in a reasonable timeframe:** Developers spend a considerable amount of resources and effort to ensure the security functions of their product work as advertised. Our experience is that it is a rare occasion where a CC evaluation uncovers a bug or flaw that would allow an attacker to bypass a security mechanism or render the mechanism unable to enforce its design goals. It is well understood and accepted that these products contain flaws/vulnerabilities that can be exploited by attackers. This is true regardless of any certification the product may have undergone. This technology class is simply too large and complex for an independent assessment to be performed that is comprehensive and complete.

It is our opinion that an objective and repeatable CC GPOS evaluation cannot be accomplished using current practices. Given the results of such an evaluation are suspect and do not provide our customers value, it does not warrant the resources expended by performing technical oversight of evaluations of this nature. Therefore, at this time, we do not support the creation of a cPP for this technology class, nor would we indicate any preference regarding procurement of GPOS products that underwent an evaluation against a cPP.

**Future:**
While we reject the concept of evaluating GPOS products using the traditional monolithic approach, we believe that cannot simply ignore this technology class. As described above, GPOSs serve many purposes, including providing a platform for important applications. We are currently exploring approaches that would allow us to make meaningful statements that are relevant to our customer’s needs. One approach is to examine specific security functions that a GPOS provides, such as a VPN client, a Wireless client, or full disk encryption. Another approach is to consider how applications use the GPOS platform and evaluates the use of these services, such as cryptographic primitives, cryptographic protocols, and protection mechanisms such as data execution protection. Yet another consideration to the OS problem space is the growing proliferation of mobile devices. While these operating systems can be just as complex as the GPOS, developers and service providers attempt to restrict the visibility of those interfaces to untrusted users. It is not clear how successful these attempts will be in the long term. Another issue with this class of products is the speed of the development cycle.

We are determined to face these challenges in a way that satisfies our customer’s needs, while still adhering to the principles expressed in the CCMC Vision Statement. There may not be a single approach to addressing these issues, and we are determined to work with the OS developers, and the CCRA Participants, to develop sensible strategies to address this very important technology class.