From: Houck, Carol S
Sent: Wednesday, May 11, 2011 11:11 AM
To:
Subject: Publications and Future Support for Separation Kernels

All

The Information Assurance Directorate (IAD) of the National Security Agency (NSA) published the current version of the U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness (SKPP) through the National Information Assurance Partnership (NIAP) in2007. The SKPP collected requirements and guidance for a small, specialized operating system kernel that would focus on tightly controlling information flow in a system, thereby facilitating the use of rigorous assurance evidence in the kernel itself and, it was hoped, supporting the assurance of the systems in which the kernel would be embedded.

Unfortunately, the commercial ground has shifted faster than we anticipated and our efforts to support existing SKPP evaluations have revealed a number of difficulties in the areas of assurance maintenance, scalability, cost and complexity when applied to complex commodity platforms. Because the SKPP has its sights on a risky and difficult environment (High Robustness), the significance of these issues requires a new strategy. It is important for the community to understand and contribute to a resolution of these issues. To facilitate this, IAD has published a document based on analysis of SKPP assurance maintenance by IAD's System and Network Analysis Center (SNAC). This document, titled "Separation Kernels on Commodity Workstations" is attached and will soon be available at the following URL:

www.nsa.gov/ia/guidance/system_level_ia_guidance/index.shtml

The conclusions of the SNAC, as outlined in the above document, indicate that the current methods for assessing and providing assurance for a Separation Kernel do not scale on complex commodity systems and a new paradigm is required. The coincides with changes in the IAP that also address common misperceptions regarding assurance and evaluation – higher EAL (usually at higher cost) does not necessarily translate into a more secure system and can significantly drain resources. Both of these new NSA efforts require community involvement. In order to understand and assess complex commodity platforms, evaluation organizations will require support from companies that develop every layer of a system (platform, operating system, middleware, applications, etc.). These layers cannot adequately be addressed in isolation; the security arguments of the system must compose into a cohesive, convincing argument for the system as a whole. This will require cooperation between NSA and numerous industry partners.

In order to begin this collaborative endeavor, IAD is also publishing a short summary of questions and answers on the topic of SKPP and High Robustness. This document outlines NSA's current position in addressing these issues. However, this is just a starting point. Continued collaboration with industry and government partners will lead to better solutions. The summary can be found at the following URL:

www.nsa.gov/ia/guidance/system_level_ia_guidance/index.shtml

Essentially, the previous strategy for NIAP evaluation against the SKPP will be replaced by direct support to the Certification and Accreditation (C&A) process for critical systems, including early design stages as well as final testing and operation. In providing this support NSA will focus on improving the security

posture of current systems even as the future improvements are just beginning to be designed. Evidence may be reused across different evaluations, as appropriate, but the focus will be on the specific system's entire security argument. (For example, SKPP certification of the kernel in a cross-domain solution is irrelevant if the system fails to filter transferred data as the application layer.)

In order to devote NSA resources to directly supporting the C&A process, the NIAP will sunset the SKPP on June 1, 2011. While currently active evaluations may complete, no further evaluations against the SKPP will be accepted, and assurance maintenance will only be accepted for minor changes for 2 years following the product certification date. Nonetheless, the content and spirit of the SKPP will continue to drive the creation of assurance arguments and evidence. Instead of using this effort on a generic Target of Evaluation, it will be directly applied to real systems.

There may be some difficulties in the transition from the previous NIAP process, but IAD is committed to improving the security posture of critical systems. This required continuing collaboration with partners in government and industry, and we appreciate the opportunity to work together toward the goal of constantly improving security. Many partners already have NSA points of contact through the NSA/CSS Commercial Solutions Center. Further, direct discussion on these issues can be coordinated through those channels. In additional questions and comments can be directed to Margaret Salter, NSA/IAD Vulnerability Analysis and Operations Technical Director, at 410-854-7087 or misalte@nsa.gov

Very respectfully,
Carol

Carol Saulsbury Houck
Director, NIAP
National Information Assurance Partnership
NSA Commercial Solutions Center (NCSC)
9800 Savage Rd., Suite 6757
Ft. Meade, MD 20755-6757
Phone: 410-854-4458
FAX: 410-854-6615
Email: cshouck@missi.ncsc.mil
Website: www.niap-ccevs.org