Common Criteria Protection Profiles—Addressing Diverse Constituencies

Gary Stoneburner, Panel Chair, NIST, CS2 PP
This year NIST produced a new version of the CS2 profile for commercial off-the-shelf (COTS) information technology. This profile is CC version 2 compliant; establishes requirements for distributed, near-term achievable COTS with a low evaluation cost; and applies to operating systems, applications, and networking. Key design goals were (1) selecting requirements that do not require significant changes to current, best commercial development practices and (2) accurately describing the security that compliant devices can be reasonably expected to provide.

Wayne Jansen, NIST - Firewall PPs
Last year, NIST and NSA jointly developed two distinct, CC version 1.0, protection profiles defining the basic security requirements for firewalls protecting unclassified information in low risk environments. The first, a profile for traffic filters, applies to devices that are capable of screening traffic at the network and transport protocol levels. The second is for application level firewalls and applies to devices that are capable of screening application protocol traffic, in addition to the network and transport levels, and authenticating end-users.

Jeff DeMello, Oracle, DBMS PPs
Oracle has developed two DBMS PPs, a Commercial Database Management System PP (C.DBMS PP) and a Government Database Management System PP (G.DBMS PP). C.DBMS PP was developed directly from the existing Security Target for Oracle's ITSEC evaluation of Oracle 7 as a "test case" with a previously evaluated product to gain experience with a CC evaluation. G.DBMS PP is a generic PP (i.e., no Oracle specific claims) intended as a baseline for all DB vendors wanting to meet TCSEC C2 or ITSEC F-C2/E2 requirements.

R. "Mouli" Chandramouli, NIST, RBAC PP
The development of a PP for role-based access control (RBAC) brought to the fore several issues with regard to the PP development process in general and specifically to the development of an RBAC PP. Some of them are: (a) the correct level of granularity for a PP, (b) the necessity of a PP for a particular security mechanism/paradigm, (c) the formulation of threats and objectives for multiple heterogeneous environments, and (d) the selection of a minimal set of mandatory features for RBAC, considering that there are several RBAC models with varying features.

Marc Laroche, Entrust Technologies, PKI STs
Entrust Technologies has prepared Security Targets (STs) for the Common Criteria evaluation of its Public Key Infrastructure core components, i.e. Entrust/Authority and Entrust/Admin. The STs are aligned with the CS2 Protection Profile (PP) and fully comply with the assurance requirements of the CS2. I intend to discuss the experience that we have gained with the development of these STs and the importance of having meaningful PPs in the world of IT security.