

The Relationship of System & Product Specifications and Evaluations

Marshall D. Abrams
The MITRE Corporation
abrams@mitre.org

1. Security property determination

The security properties of Information Technology (IT) products and systems are important to the national security, critical infrastructure, and economic health of advanced society. These properties are studied, tested, and evaluated to provide information for decisions concerning trustworthiness and suitability for purpose.

This panel will address present and future approaches to these determinations. Following panelist's opening statements the moderator will ask important provocative questions and accept questions from the audience. The following questions are indicative of the discussion.

1. There appears to be a paradigm shift in process. What is happening in and between the schemes described below and similar activities in other sectors?

2. All organizations have resource limitations (e.g., skill, time, money). What are the most cost-effective activities in improving the security of IT products and systems using in the normal conduct of enterprise business, in critical infrastructure, and in national defense?

3. Systems involve multiple products, integrators, evaluated products, "glueware" that melds the products into systems. Should efforts focus on the weakest links? What can be done? How can information gained in each activity be reused?

2. Acquisition and the security communities

For years the acquisition community and the security community have struggled to come together in a fashion that would result in successful procurement of very large systems with appropriate security properties. A major issue has often been that the security engineers articulated their design using their own paradigm and language while the acquisition community procured systems and components using a different paradigm and language. Only at the very highest levels of reference has the procurement paradigm and security community language come together in an attempt to acquire secure systems. Even at this highest level of specification, most procurement

strategies have been based on product level specification without consideration of the security properties of the system as a whole.

3. Specification of security properties

In principle the specification of security properties should be no different than the specification of other properties of the system. One should anticipate typical conflicts among specifications and goals. Trade-offs will have to be made when all specifications and goals cannot be achieved. The customer will be involved in some of the decisions concerning trade-offs and will help the integrator decide how to evolve the specifications and goals as well as the system.

The International Standard ISO/IEC 15408 [1], the Common Criteria (CC) for Information Technology Security Evaluation, provides a model for specifying and evaluating security properties of COTS products and small systems.

The US is represented within the CC Project by the National Information Assurance Partnership (NIAP), a joint National Institute of Standards and Technology (NIST) and National Security Agency (NSA) project. NIAP, in turn, has established the Common Criteria Evaluation and Validation Scheme (CCEVS) to implement the Common Criteria Recognition Arrangement (CCRA) compliant evaluation scheme within the US. [2] In September 2002, NIAP held a workshop *Integrating Security into Large-scale Acquisitions*.

4. Federal Information Security Management Act

NIST is conducting a program mandated by the Federal Information Security Management Act including security categorization of information and information systems; selection of appropriate security controls for information systems; verification of security control effectiveness and determination of information system vulnerabilities; and operational authorization for processing (security accreditation) of information systems. The intended outcome includes more consistent, comparable, and repeatable

evaluations of security controls applied to information systems; a better understanding of enterprise-wide mission risks resulting from the operation of information systems; more complete, reliable, and trustworthy information for authorizing officials—facilitating more informed security accreditation decisions; and more secure information systems within the Federal government including the critical infrastructure of the United States.

5. References

[1] Common Criteria Project, Common Criteria for Information Technology Security Evaluation, version 2.1 (1999). Or, International Standard ISO/IEC 15408 (1999-12); Parts 1-3, Information Technology Security Techniques Common Criteria for IT Security Evaluation (CCITSE). Available from: <http://csrc.nist.gov/cc/>.

[2] *Common Criteria Evaluation and Validation Scheme (CCEVS)*. Available from <http://niap.nist.gov/cc-scheme/>.