Abstract for proposed submission
to
Fourth Workshop on Distributed Object Computing Security

"Using the Common Criteria and the National Information Assurance Partnership to Establish DOCsec Product Trust and to Enhance International Markets"

by

Stuart Katzke, Chief Scientist
Information Assurance Solutions Group
National Security Agency,
swkatzk@missi.ncsc.mil

As various industry sectors incorporate Distributed Object Computing (DOC) into their operations and business models, trust in the quality of the security features implemented in DOC IT environments becomes essential for new DOC IT-based approaches to flourish. To achieve this trust, it is necessary to define the functional security requirements of DOC IT products, as well as, the desired level of confidence that the products meets the functional security requirements. Even more daunting is how to develop trust and confidence about composite enterprise security solutions created by integrating individual DOCsec products with other types of products.

The Common Criteria standard (ISO 15408) provides a solution to these problems. It is an internationally-accepted, standard language and method for stipulating requirements and specifications of security functionality and assurance. In addition, accredited, commercial Common Criteria security evaluation laboratories around the world are now available and use standard Common Criteria evaluation methodology to evaluate, in a comparable way, the security and assurance claims of IT products and systems specified in accordance with the Common Criteria standard. Furthermore, due to Common Criteria Mutual Recognition Arrangements (CC MRA) among the governments of many of the world's largest IT building and buying countries, IT products evaluated by such accredited testing laboratories in any one country are recognized without any further re-testing in all other countries.

Realizing the common benefits afforded by the Common Criteria security specification and evaluation paradigm, several industry sectors are now embracing them. The financial communities' smart card issuing sector is moving quickly to adopt Common Criteria specifications and to outsource card testing to the Common Criteria testing laboratories. The healthcare industry is looking to use the Common Criteria approach to solve its needs to validate IT product compliance to new federal privacy and security regulations. The telecommunications industry is also now turning its attention to the Common Criteria. The benefits being realized are many and make powerful arguments about the value of the Common Criteria approach to the DOCsec marketplace.

Dr. Katzke will discuss how the Common Criteria scheme for specifying and evaluating security can establish trust in the security capabilities of DOCsec IT products. This is accomplished through independent verification that IT products and systems behave reliably and to specification. IT purchasers will gain confidence that the products they buy are providing appropriate levels of protection and that their reliance on such best-available industry practices can add to evidence of their due diligence in providing adequate security solutions. The benefits currently being derived by communities embracing the Common Criteria will be discussed.