An Evaluation and Certification Scheme for MILS

Rance J. DeLong*
The Open Group

Abstract

Over the past decade there has been steady activity and progress associated with MILS, a modular or "compositional" approach to the design and assurance of dependable systems [BDRS08, AFHOT06, VBC+05]. The idea is that the assured properties of MILS components have a form that allows the assurance of a MILS system to be based largely on that of its components [Rus08]. A coalition of vendors, government customers, system integrators and academics, referred to as the *MILS Initiative*, is actively seeking to build high-assurance systems on a foundation of standardized high-assurance components, and to establish a COTS market for those components.

The technical and commercial success of MILS is contingent on time- and cost-effective processes for evaluation of MILS components, and for compositional certification of systems built with those components [DR09, DeL09]. These evaluation and certification processes must be suited to a global marketplace, where component vendors, system integrators, and customers may be from different countries. Currently, security evaluation is performed by national schemes which, though all based on the Common Criteria [CC309, CEM09], differ in their approach to high-assurance evaluations and in their treatment of high-assurance evaluations performed by other nations.

The Open Group is considering establishing a new, independent MILS evaluation and certification scheme based on the Common Criteria, augmented by MILS compositional assurance theory and explicit argument-based assurance cases. Based on open standards and a rigorous methodology, the scheme will serve the interests of customers and system integrators, while benefitting the vendors of MILS products and services, by offering uniform and trustworthy state-of-the-art technical assessment services. This open scheme avoids the cost and pitfalls of garnering the acceptance of each national scheme, while its argument-based assurance case provides all the information needed for review by a national scheme.

The Open Group is not new to MILS. The Real Time & Embedded Systems Forum of The Open Group has long been a focal point of MILS activity. Leveraging its reputation and integrity as an international standards body, The Open Group would provide the standards and governance for the new scheme and serve as its certifying body, providing a basis for international recognition of high-assurance MILS components and systems. Just as open standards have enabled competition and a corresponding rapid growth in quality and diversity of traditional products and services, so an open and compositional argument-based approach to evaluation will spur development of high-assurance products and services.

*Rance DeLong is a consultant, staff scientist at LynuxWorks, and adjunct lecturer at Santa Clara University.

Community Investment in MILS

Over the decade, the MILS[1] community has made an enormous investment of time and money, motivated by the compelling prospects for MILS. Over that period of time there have been significant constants: stalwart leadership and investment in MILS technology research by government, commitment to the MILS approach by industry as demonstrated within The Open Group's Real Time & Embedded Systems Forum, growing interest on the part of potential government and commercial MILS customers, and continuing investments in MILS products by vendors.

Through research and development contracts, the U.S. Air Force has sponsored the refinement of MILS concepts, development of MILS middleware, definition of MILS component protection profiles, conduct of foundational research, and articulation of the MILS vision and roadmap.

Product vendors, including, Green Hills, LynuxWorks, Objective Interface Systems, Real-Time Innovations, and Wind River, have invested heavily in involvement in the MILS community and development of MILS products.

System integrators, including, Boeing, General Dynamics, Lockheed Martin, Northrop Grumman, Raytheon, and Rockwell Collins, have developed and/or proposed solutions based on MILS, have encouraged the pursuit of MILS through their involvement in forums such as The Open Group, and have independently invested in the development and application of MILS technology.

Need for a MILS Evaluation and Certification Scheme

We refer to the technical assessment of MILS *products* as "evaluation," and to the technical assessment of MILS-based *systems* as "certification."[2] Subsequent to certification, systems will typically undergo a risk-based assessment, considering the results of certification, to decide whether to grant approval to operate the system in a specific operational environment.

The success of MILS is critically dependent on a responsive and trustworthy evaluation and certification scheme for components and systems. Trust in the *MILS certifying body* is key to acceptance and international mutual recognition of evaluation and certification results. This is particularly germane to *high assurance* evaluation and certification. Timely response to evaluation and certification needs are critical both to the vendors and consumers of MILS products.

Because MILS advances the state of the art in both technical and certification dimensions, MILS is dependent on a progressive evaluation and certification scheme. The scheme must deliver uniform and trustworthy results consistent with the Common Criteria (CC), which provides the framework for the expression of MILS component and system security requirements, and with augmented standards and methodology specific to MILS. Laboratories already accredited to perform CC evaluations could additionally demonstrate proficiency and be accredited for the MILS evaluation methodology. It will be a function of the MILS Evaluation and Certification Scheme to accredit laboratories to perform MILS evaluation and certification activities.

To date, international standards such as the CC have experienced less than complete success in achieving timely, trustworthy, affordable, repeatable and internationally-recognized evaluations.Virtually all product evaluation and system certification assessments are performed by national agencies, each applying their own nuances, complicating international acceptance.

[1] "MILS" was originally an acronym for Multiple Independent Levels of Security. Today, we use "MILS" as a proper name for an architectural approach promulgated by the *MILS Initiative*, a collective of vendors, system integrators, researchers, educators, and government workers, and as elaborated by ongoing MILS research efforts.

[2] "Evaluation" and "certification" are overloaded terms, with conflicting definitions in different communities. In addition to abuses particular to each term, the two are also often equated, which they should not be.

If MILS were to depend on the existing schemes, the MILS community would need to educate and win acceptance by each scheme one at a time, a laborious undertaking unlikely to succeed. National schemes may adopt individual policies that render them unpredictable to provide even the basic CC evaluation services required to support MILS evaluation and certification. The additional technical requirements for MILS evaluation and certification make it an unpromising strategy to rely on the existing schemes to achieve widespread uniform application and internationally acceptable results. Some system certification regimes have failed to effectively utilize the CC by not requiring evaluation of component products, thereby losing the industry-wide leverage that comes with the availability of evaluated off-the-shelf products, a key tenet of MILS.

Finally, the success of MILS evaluation and certification would be facilitated by a constructive and cooperative relationship between the product developers and system architects on the one hand, and the product evaluators and system certifiers on the other hand. While the evaluators and certifiers are required absolutely to maintain strict objective standards of achievement, the entire process can yield better results in a more cost-effective way if there is a constructive and supportive interaction. For high assurance product evaluation and system certification the evaluation and certification process will best span the entire product or system development activity. Guidance from evaluators and certifiers should be provided as needed throughout the development cycle to avoid costly backtracking, and the pressure to accept products or systems that are deficient because it is too late to actually fix them.

Organization of a MILS Evaluation and Certification Scheme

The MILS Evaluation and Certification Scheme ("MILS Scheme") is concerned with the evaluation of MILS products against their requirements and with the composition of evaluated MILS products into systems. It is concerned with the inference properties of the system from the properties of components. Since only some of the properties of concern for MILS systems are security properties, the CC by itself is not sufficient to encompass MILS. However, the MILS Scheme would leverage the CC to the greatest extent practical. It is by no means hostile to the CC or in conflict with the CC. In fact, the MILS Scheme embraces the CC and meshes well with it and with the Common Criteria Recognition Agreement (CCRA) as discussed in the final section.

Evaluation and certification activities under the MILS Scheme can be identified with one of two domains, a CC domain and a MILS domain. The CC domain covers protection profiles, security targets, and TOE evaluations that relate to the security problems and solutions that can be described within the CC framework, including those achievable with extensions that are consistent with the CC, and can be conducted within established CC practice. The MILS domain includes MILS architecture, MILS compositional theory, MILS component interoperability, MILS compositional certification, and MILS enhanced assurance requirements. These things are either not addressed by the CC or are not adequately addressed for MILS by the CC.

The boundary between the CC domain and the MILS domain is both permeable and changeable. Concepts and practices from the MILS Scheme that may be adopted in the future by the CC would move from the MILS domain into the CC domain. New developments in the CC domain could influence the MILS domain, as the MILS Scheme attempts to maintain maximum practical leverage of the CC.

The Open Group (TOG) seeks to establish the proposed Scheme for MILS product evaluation and MILS system certification support. The MILS Scheme would be based on a faithful application of the Common Criteria, applying the general standards, practices, and guidelines

established for the Common Criteria. TOG would apply to become a CC Certificate Authorizing Scheme, and would seek representation on the CC Development Board. The MILS Scheme will rely upon CC approved licensed evaluation laboratories to perform the CC domain aspects of MILS evaluation and certification. TOG, as the certifying body for the MILS Scheme, would provide accreditation of evaluation laboratories, upon demonstration of proficiency, to perform the additional MILS-specific evaluation and certification activities.

MILS Product Evaluation and System Certification

Product evaluation and system certification are distinct activities, but in MILS they share common foundations, and the objectives of MILS span both activities. Independently developed and evaluated MILS components are intended to enable composable systems and compositional system certification. To achieve the fullest measure of success for MILS, it is necessary that both functional and assurance composition objectives succeed.

MILS product evaluation is based on standards that include MILS protection profiles (PPs) for a set of MILS *foundational components* and MILS *operational components*. In addition to the separation kernel [Rus81, SKP07], MILS foundational components include a console system, a network system, and a file system. Operational components include a generic guard/downgrader. The allocation of function to, and the specific trust obligations among the MILS components is specified by the MILS Integration Protection Profile (MIPP), to which each of the MILS PPs claims conformance.

Vendor-authored security targets (STs) for independently developed MILS components should claim conformance to the corresponding MILS protection profile, thus inheriting the MIPP-specified requirements. Such STs and targets of evaluation (TOEs), as well as the MILS protection profiles themselves, will be evaluated under the MILS Scheme.

MILS system certification support provided under the Scheme could provide a substantial portion of the overall technical effort required for the certification and accreditation of a MILS-based system. This service is not intended to usurp the authority of existing certification and accreditation regimes, nor as a substitute for the risk management-based process that a designated approving authority (DAA) typically employs to reach the decision to operate a particular system. Rather, MILS certification support would provide consistent and modular technical assessment of the MILS-specific aspects of a system. Specialized MILS architectural decomposition, evidence-based compositional assurance methodology, and automation being defined by ongoing MILS research could to enable MILS qualified developers, evaluators and certifiers to substantially improve the quality of assurance while saving on the cost of system (re-)certification.

In addition to the Common Criteria, the MILS evaluation and certification scheme will rely on technical augmentations to facilitate high-assurance evaluation and certification, including,

- an assurance case that explicitly links product claims to product-based evidence
- pervasive use of formal methods to increase rigor and confidence
- extensive use of tools and automation to diminish labor and increase repeatability
- hierarchical augmentations to the CC in support of assurance and composition
- interoperability standards for functional composability

with the goal of making high-assurance evaluation objectively verifiable and more cost-effective.

Benefits of the MILS Scheme

The Open Group believes that many benefits will accrue from the establishment of an independent certifying body, and an international evaluation and certification scheme for MILS, including,

- specialization of evaluation and certification methodology to the novel and progressive attributes of MILS
- uniform application of MILS theory, technology, and standards world-wide
- constructive and supportive collaboration with developers throughout the development and evaluation cycle to foster success rather than frustration
- trustworthy and timely delivery of evaluation and certification services
- consistent accreditation of MILS evaluation and certification laboratories
- objective basis for international mutual recognition of high-assurance results

fostering a global marketplace of standardized high-assurance MILS components.

Relationship to other Standards Bodies and Evaluation Schemes

Consistent with the philosophy of The Open Group, the MILS Evaluation and Certification Scheme will leverage existing standards, for example, using the Object Management Group's (OMG) metamodels for evidence and argumentation in the explicit assurance cases proposed for MILS evaluation and certification. The Scheme will leverage the willing assistance of other institutions able to substantively contribute expertise or support, while maintaining the independence and focus of the MILS Scheme, and avoiding any perceived or actual relationship that would detract from the effectiveness or trustworthiness of the MILS Evaluation and Certification Scheme.

The proposed MILS Evaluation and Certification Scheme would apply the International Common Criteria faithfully. Augmentations by the MILS Scheme would be formulated as proper extensions to the CC. The Scheme would contribute its experiences in the MILS arena to help improve the CC in the future. The MILS Scheme, providing evaluations only above evaluation assurance level 4 (EAL 4), would be strictly complementary to the existing Common Criteria Recognition Agreement (CCRA), subscribed to by 25 countries, which provides mutual recognition only up to EAL 4. Another progressive Mutual Recognition Agreement, subscribed to by 10 European countries, known as the SOG-IS Agreement (Senior Officials Group Information Systems Security), provides mutual recognition up to EAL 7. The Open Group is interested in exploring collaboration with SOG-IS to establish a wider framework of participation to include a commercial scheme.

The MILS Scheme would enable the MILS Community to follow through on its substantial MILS investment. The MILS Scheme does not seek to compete with existing national schemes, but to provide unique supplementary services that promote the success of MILS for its international community of providers and customers alike, and is conceived in the spirit of international cooperation.

References

[AFHOT06] Jim Alves-Foss, W. Scott Harrison, Paul Oman, and Carol Taylor. The MILS architecture for high-assurance embedded systems. *International Journal of Embedded Systems*, 2(3/4):239–247, 2006.

[BDRS08] Carolyn Boettcher, Rance DeLong, John Rushby, and Wilmar Sifre. The MILS Component Integration Approach to Secure Information Sharing. In *27th AIAA/IEEE Digital Avionics Systems Conference*, St. Paul, MN, October 2008.

[CC309] *Common Criteria for Information Technology Security Evaluation*, July 2009. Version 3.1 Revision 3, CCMB-2009-07-001, 002, 003.

[CEM09] *Common Methodology for Information Technology Security Evaluation*, July 2009. Version 3.1 Revision 3, CCMB-2009-07-004.

[DeL09] Rance DeLong. Compositional Certification Lecture Notes. October 2009.

[DR09] Rance DeLong and John Rushby. Compositional Certification. In *HAMES Project Year End Review*, El Segundo, California, October 2009.

[Rus81] John Rushby. The Design and Verification of Secure Systems. In *Eighth ACM Symposium on Operating System Principles*, pages 12–21, Asilomar, CA, December 1981. (ACM *Operating Systems Review*, Vol. 15, No. 5).

[Rus08] John Rushby. Separation and integration in MILS (The MILS Constitution). Technical report, Computer Science Laboratory, SRI International, Menlo Park, CA, February 2008.

[SKP07] Information Assurance Directorate, National Security Agency, Fort George G. Meade, MD 20755-6000. *U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness*, June 2007. Version 1.03.

[VBC+05] W. M. Vanfleet, R. W. Beckwith, B. Calloni, J. A. Luke, C. Taylor, and G. Uchenick. MILS: architecture for high assurance embedded computing. *CrossTalk*, 18:12–16, August 2005.