An Evaluation and Certification Scheme for MILS

Rance DeLong*
The Open Group

Layered Assurance Workshop
December 2010

* Rance DeLong is a Consultant, Staff Scientist at LynuxWorks, and an Adjunct Professor at SCU.

Overview

- Steady investment and progress in MILS over the decade
- Shared vision and objectives: a global MILS marketplace of products enabling composable dependable systems
- Technical and commercial success dependent on an efficient process for product evaluation and system certification
- Existing CC-based national schemes differ in their approach to high assurance evaluations and international recognition
- The Open Group is exploring the establishment of a new, independent MILS evaluation and certification scheme
  - Based on the Common Criteria and open standards
  - Augmented with MILS specific technology & evaluation methodology
- Best strategy for realization of MILS vision
  - Centralizes MILS governance, technology and evaluation oversight
  - Avoid serial proselytizing of national schemes
  - Most responsive to needs of MILS and fosters the MILS marketplace

Investment in MILS

- MILS prospects have motivated an enormous investment
- MILS and MILS-related research investment by government
- MILS promotional investment by government, vendors and system integrators (SIs)
- MILS product development investment by vendors
- MILS infrastructure and middleware investment by vendors and SIs
- MILS approach investigation and adoption by SIs and customers

Need for MILS Eval. and Cert. Scheme

- Terms - how they're being used here:
  - Evaluation - technical assessment of MILS products to CC and MILS standards
  - Certification - technical assessment of MILS-based composite systems
  - System Certification & Accreditation (C&A) - a technical and risk-based assessment used to reach a decision to deny or approve a system to operate
- Success of MILS is critically dependent on a responsive and trustworthy evaluation and certification scheme
  - MILS is seeking a more comprehensive result than common practice
  - Must incorporate MILS-specific technology and methods
  - Transparent and repeatable methodology to foster increased trust
  - Timely evaluation and certification essential to vendors and users
- "MILS consumers" are relying on "MILS producers" to deliver

Need for MILS Eval. and Cert. Scheme

- Dependence on existing Schemes is intractable
  - Educating and winning acceptance one-scheme-at-a-time
  - Not a path to uniformity of application or results
  - CC, despite shortcomings that may be attributed to it, is not being effectively and uniformly used everywhere
- Constructive and cooperative relationship among developers and evaluators would facilitate MILS success
  - Evaluation spans product development process
  - Certification spans system development process
  - Avoids costly backtracking
  - Avoids tendency to accept something that's "too late to fix"

Approach

- TOG to establish an ***independent Scheme for MILS product evaluation and MILS system certification support***
  - Product evaluation and system certification are distinct activities
  - In MILS these share common foundations
  - MILS objectives span both of these activities
    - MILS components intended to achieve composable systems and compositional system certification
- MILS component evaluation
  - MILS foundational component PPs and the MILS Integration PP
  - MILS operational component PPs
  - Vendor's PP-conformant STs and TOEs evaluated by the Scheme
  - Based on Common Criteria plus MILS augmentation
- MILS compositional system certification *support*
  - Not intended to usurp authority of existing C&A regimes
  - Provide assessment of MILS-specific aspects of a system *effectively*
  - Existing C&A regimes decide the weight to be given MILS certification

Approach - CC and MILS Domains

- CC Domain
  - Use the “vanilla” Common Criteria to greatest extent practical
  - MILS-specific extensions to the CC
    - Attempt first to do as proper extensions to CC, e.g., MIPP, polymorphic protection profiles shown to be able to be evaluated using CEM
    - Added rigor for high assurance PPs
- MILS Domain
  - MILS-specific, e.g., Assurance cases (Claims-Argument-Evidence Model)
  - MILS standards, e.g., APIs, interoperability standards
  - MILS compositional certification theory and practice
  - Other properties of concern in addition to Security covered by CC Domain
- CC Domain / MILS Domain Boundary
  - Permeable and changeable over time
  - MILS Domain developments will be submitted to future CC conferences
    - Help to shape future directions of the CC, esp. for high assurance
  - New developments in the CC Domain
    - If these come from inputs to CC from MILS Domain then they migrate from MILS to CC Domain
    - May influence changes in MILS evaluation approach

Approach - Criteria and Methodology

- Apply the international CC faithfully (be a good CC citizen)
  - Use the CC fully and consistently
  - MILS' EALs 5-7 does not conflict with CCRA (EALs 1-4) !
  - Apply for recognition by the CC community (CCMB)
  - Participate in the ongoing development of the CC (CCDB)
- Augment with MILS-specific technical measures and methodology to support high-assurance evaluation and certification
  - Assurance case - linking product claims to product-based evidence
  - Pervasive use of automated formal methods to increase rigor
  - Tools to diminish labor and increase repeatability
  - Augmentation to CC supporting high assurance and composition
  - Polymorphic PPs and high-assurance augmented PPs
  - Interoperability standards for functional composability
- Make high-assurance evaluation objectively verifiable and more cost-effective

Benefits

- Specialization of evaluation and certification methodology to the novel and progressive attributes of MILS
- Uniform application of MILS theory, technology, and standards
- Constructive and supportive collaboration between evaluators and developers throughout development and evaluation cycle
- Trustworthy and timely delivery of evaluation and certification services
- Consistent accreditation of MILS-qualified evaluation and certification laboratories (extending existing CCTLs)
- Objective basis for international mutual recognition of high assurance results
- Foster the global marketplace of standardized high-assurance MILS components

Relationship to other bodies and schemes

- Use existing standards, e.g., TOG, OMG, IEEE, ISO, etc. where applicable and reasonable
- Develop new TOG standards for MILS as needed, e.g., MILS API Standard, MILS Separation Kernel annex, MILS interoperability standards
- Enlist the willing assistance of existing institutions and services, e.g., NIST, worldwide Common Criteria Testing Laboratories (CCTLs)
- Apply the CC as a new CC scheme and participate in future development of the CC, contributing the benefits of the MILS experience
- Does not seek to compete with CCRA schemes
- Seek alignment with other mutual recognition arrangements that provide international recognition of high assurance levels

References

[1] 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, Oct 2008, awarded *Best of Conference* at 2009 DASC.

[2] John Rushby. Separation and Integration in MILS (The MILS Constitution). Technical Report, Computer Science Laboratory, SRI International, Menlo Park, CA, Feb 2008.

[3] John Rushby. A MILS Example. Technical Report, Computer Science Laboratory, SRI International, Menlo Park, CA, May 2009.

[4] Rance DeLong and John Rushby. High-Assurance Development and Evaluation: Rethinking the Common Criteria and EAL 7. 9th International Common Criteria Conference, Jeju, Korea, 2008.

[5] Rance DeLong. Polymorphic Protection Profiles. 11th International Common Criteria Conference, Antalya, Turkey, 2010.