PNNL-13587

Authentication Assurance Levels: A Strategy for Applying the ISO Common Criteria Standards

R.T. Kouzes
J.R. Cash
D.M. DeVaney
B.D. Geelhood
R.R. Hansen
R.B. Melton

July 23, 2001 Revision 0.6

Prepared for
The U. S. Department of Energy
Under Contract DE-AC06-76RLO 1830

Pacific Northwest National Laboratory

Richland, Washington 99352

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-ACO6-76RL0183O

Printed in the United States of America

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov

Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm

PNNL-13587

Authentication Assurance Levels: A Strategy for Applying the ISO Common Criteria Standards[1]

RT Kouzes
JR Cash
DM DeVaney
BD Geelhood
RR Hansen
RB Melton

July 23, 2001 Revision 0.6

Prepared for
The U. S. Department of Energy

Pacific Northwest National Laboratory

Richland, WA 99352

[1] This paper is one of four documents developed by PNNL that introduce the application of the CC to authentication:

Authentication Assurance Levels: A Strategy for Applying The ISO Common Criteria Standards
Authentication Assurance Level Application to the Inventory Sampling Measurement System
A Review of the IAEA Vulnerability Assessment Level Scheme: Applicability to DTRA and DOE Programs in the FSU
Inventory System Measurement System Common Criteria Authentication Protection Profile

SUMMARY

The Common Criteria (CC) is an internationally recognized, multi-part standard for the evaluation of security properties within Information Technology products or systems. The CC provides a set of composition rules to develop a rational and repeatable graded assurance package. This graded assurance package establishes a set of levels composed of criteria for evaluating a system or product. As the levels increase, the assurance that a product meets the security and functional requirements also increases. Since the CC only provides a set of composition rules, the final set of evaluation levels can be modified to meet the specific needs of an application. This Common Criteria approach is applied here to create a definition of *Authentication Assurance Levels* (AALs) that can quantify the level of assurance reached for a system subject to a set of authentication procedures.

INTRODUCTION

This paper focuses on articulating a graded scale approach for authentication activities associated with monitoring equipment in non-proliferation and arms-reduction regimes. The concept of *Authentication Assurance Levels* (AALs) is introduced to address the unique assurance requirements for monitoring systems being developed by members of the Former Soviet Union (FSU), especially the Russian Federation (RF). These monitoring systems are being developed in support of a range of arms-reduction negotiations to indicate compliance with the disassembly and storage of nuclear weapons and weapons materials. Authentication, certification, and demonstration of operational functionality are all typically required for a viable monitoring system. The basic authentication requirements are that a monitoring system be able to make the required measurement(s), that the system function as designed, and that there be no hidden features in the system that allow the results to be altered. [Geelhood 2000]

We believe that the Common Criteria (CC) [ISO 1999] is an appropriate tool to articulate the requirements for security properties that should be included throughout the lifecycle of a monitoring system. The framework and security criteria presented in the CC provide a good foundation for developing appropriate assurance measures that a system functions properly and does not contain a hidden feature. The reasons we recommend that authentication activities be based on a modified CC approach are:

- The CC has been adopted as an international standard, created to produce consistent and believable results that could cross international boundaries.
- The CC provides a set of composition rules to develop an appropriate and complete set of assurance levels, ensuring that all security and authentication issues are identified, communicated, and resolved.
- The assurance levels provide a graded approach with quantified measurable results.
- The standard framework and resulting assurance level criteria ensures the authentication process can be repeatedly performed in a consistent manner.

- The CC provides a standard language for communicating security requirements and assurance results between the specifying party, the developer, the evaluator, the user, and other members of the community.
- The CC addresses the security requirements without distinguishing between hardware, firmware, or software.
- Consistent with authentication philosophy, the CC bases assurance upon evaluation and active investigation.

THE COMMON CRITERIA

The CC is an internationally recognized, multi-part standard for the evaluation of security properties within Information Technology (IT) products or systems. By establishing such a common criteria base, the results of an IT security evaluation are more meaningful to a wider audience [ISO 1999]. The CC is currently supported by recognition agreements between 14 nations, and this number is growing. For example, the RF is working toward replacing their current policy for IT security with the CC, and Japan, The Netherlands, Sweden, and Israel are considering, or are in the process of becoming, CC certified producers of products or systems. [Ambuel 2001]

The recognition agreements or certification ensures that each country's scheme produces a correct and complete evaluation and that the results are presented in a consistent manner. Additionally some member states have established national policies that pertain to the CC. One example is the National Information Assurance Acquisition Policy that was issued by the United States. This policy requires that all IT and equipment that handles national security information be developed and evaluated within the framework of the CC. The use of an internationally recognized standard enhances the ability for groups developing, using, and evaluating a product to communicate, and allows the evaluation results to be more universally accepted, even across international boundaries. [IAEA 2001]

The CC strives to address the often diverse needs of three separate groups: the consumer, the developer, and the evaluator. Consumers need a usable set of results from a rigorously constructed evaluation to allow them to determine the appropriateness of a product. To help prepare for and assist in the evaluation of their product or system, developers need to be able to identify the security requirements to be satisfied. To judge the conformance of a product to a set of security requirement, evaluators need a set of criteria and a method for presenting the results in a consistent manner. [ISO 1999]

To achieve greater comparability between evaluations, the CC created a framework to define a set of standards for product evaluation. The CC also establishes a process for monitoring the quality of a product or system evaluation and provides for an independent inspection of the evaluation results. The CC provides a set of composition rules to develop a rational and repeatable graded assurance package. The graded assurance package establishes a set of levels composed of criteria for evaluating a system or product. As the levels increase the assurance that a product meets the security and functional requirements also increases. Also, as the levels increase, the quality of the developer's product must correspondingly increase to support a positive evaluation

outcome. Since the CC only provides a set of composition rules the final set of evaluation levels can be modified to meet the specific needs of an application.

The applicability of the CC is greatly enhanced since in general it does not distinguish between hardware, firmware, or software security measures. Certain topics are considered to be outside the scope of the CC because they involve specialized techniques or because they are somewhat peripheral to IT security. Some of these are: security evaluation criteria pertaining to administrative security measures not related directly to the IT security; the evaluation of technical physical aspects of IT security such as electromagnetic emanation control; the evaluation methodology and the administrative and legal framework under which the criteria may be applied by evaluation authorities; and the use of evaluation results in product or system accreditation.

The CC is composed of 3 distinct but related parts. *Part 1: Introduction and general model [ISO 1999]* develops the general model; it also develops constructs for communicating IT objectives and security requirements. These constructs are called Protection Profiles (PPs) and Security Targets (STs). *Part 2: Security functional requirements [ISO 1999]* establishes a set or catalog of recognized functional requirements enabling security requirements to be formulated in a standard and repeatable way. *Part 3: Security assurance requirements [ISO 1999]* is also a catalog, but it contains a set of assurance requirements. An important element of the third part is a predefined scale or rating system for evaluating the confidence in the security of a product or system referred to as the Evaluation Assurance Levels (EALs). [ISO 1999]

AUTHENTICATION

The CC uses the term "Evaluation" where the non-proliferation and arms-control community has defined and accepted the similar term "Authentication". We propose five assurance levels for the non-proliferation and arms-control community, called *Authentication Assurance Levels* (AAL) 0 to 4. This definition is done for clarity and to avoid confusion with the pre-existing meanings of the seven Evaluation Assurance Levels, or EALs, established by the CC.

The community has defined *Authentication* as "the process through which the monitoring party gains appropriate confidence that the information reported by a monitoring system accurately reflects the true state of the monitored item." [Kouzes 2001]

Authentication is an extremely important part of monitoring-system development. If the monitoring party cannot establish the credibility of a monitoring system through authentication, then it may be more cost effective to merely trust a host's declaration regarding the monitored items. The ability for authentication methods to be successfully applied must be designed into a system from the start, which makes the design task more difficult than merely designing a functional system. Designing for authentication is especially important in a resource-limited regime, where the potential gain from an expedient design decision should be balanced against the cost of the additional authentication effort it may produce. Procedures should allow for authentication throughout the lifecycle of a system. The extra effort of designing for authentication is

also beneficial to a developer whose product must separately undergo a security certification, as is the case with systems developed in both the US and the RF.

Authentication provides a level of assurance that measurement and monitoring systems are assembled as designed, function as designed, and do not contain hidden features that allow the passing of material inconsistent with accepted declaration. It goes beyond functional testing to thorough inspection of the hardware and software to ensure that no hidden features are present that would interfere with or preclude the correct measurement and display of results. Such a hidden feature could be software or hardware that responds to some external trigger signal and alters the correct response to a measured item. To effectively prevent hidden switch implementations, authentication should include significant independent examination of the system (and/or a duplicate) prior to installation and verifying the state of the system before each use to facilitate the joint inspection of the system.

Evaluation has been the traditional means of gaining assurance, and is the basis of the Common Criteria approach. Evaluation techniques can include, but are not limited to:

a) Analysis and checking of process(es) and procedure(s);

b) Checking that process(es) and procedure(s) are being applied;

c) Analysis of the correspondence between target of evaluation design representations;

d) Analysis of the target of evaluation design representation against the requirements;

e) Verification of proofs;

f) Analysis of guidance documents;

g) Analysis of functional tests developed and the results provided;

h) Independent functional testing;

i) Analysis for vulnerabilities (including flaw hypothesis);

j) Penetration testing. [ISO 1999]

AUTHENTICATION ASSURANCE LEVELS

Authentication Assurance Levels (AALs) are modeled after the CC's Evaluation Assurance Levels and can be described by a set of high-level guidelines. The AALs range from 0-4, with 4 being the level that provides the most confidence that the system meets its security objectives. To obtain a high level of authentication, the authenticating authority must identify all required assurance components prior to the development of a system to be authenticated and provide them to the developer to assist in designing the necessary authentication features into the system.

If developers are to produce systems that are expected to be authenticated at Authentication Assurance Level 4 or higher, significant improvements in automated

system development practice will be required. System development life cycle and quality standards similar to Integrated for Systems Engineering/Software Engineering/Integrated Product and Process Development, ISO12207, and ISO15288 should be adopted or developed at the national level. In the current economic climate, external assistance will almost certainly be required to support standards development and adoption in the RF and to train selected developers in system development practices. Such an investment under the umbrella of international nuclear non-proliferation would promote more full cooperation and good will in that sphere. We recommend that one way to accomplish this would be to initiate the formation of a bilateral US-RF Common Criteria Working Group. Under such an arrangement, the US could contract with selected Russian organizations to support appropriate activities.

The Authentication Assurance Levels provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. They are hierarchically ordered inasmuch as each higher AAL represents more assurance than all lower AALs. The increase in assurance from AAL to AAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigor, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements). Each AAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

The five Authentication Assurance Levels and their correspondence to the EALs are as follows:

AAL0 – unauthenticated	~EAL1 + EAL2 functionally and structurally tested
AAL1 – minimally authenticated	~EAL 3 methodically tested and checked
AAL2 – limited authentication	~EAL 4 methodically designed, tested and reviewed
AAL3 – critical authentication	~EAL 5 semi-formally designed and tested
AAL4 – optimal authentication	~EAL 6 verified design and tested

AAL0 (Unauthenticated) is applicable where no confidence in the correct operation can be expected due to the lack of assurance measures taken by the developer or authenticating authority. This AAL is used where, although some assurance measures might have been used, none are sufficient to provide any measure of confidence in system operations. For example, the developer does not develop, provide, or maintain any of the documentation on system design, development, and operations, nor does the developer allow members of the authenticating authority to participate in system design review, or to witness a comprehensive test of the system.

AAL1 (Minimally Authenticated) is the minimum level of assurance that any equipment used in a monitoring regime should have. Authentication at this level should provide evidence that the Target of Authentication (TOA)[2] functions in a manner consistent with its documentation, and that it provides useful protection against identified threats. Co-

[2] The CC uses the term Target of Evaluation (TOE), but TOA is used here to clearly identify the authentication purpose of the AALs.

operation of the developer is required in terms of the delivery of design information and test results. AAL1 is applicable in those circumstances where developers or users require a low level of independently assured security in the absence of ready availability of the complete development record. The developer conducts functional and high-level design testing, and independent testing is conducted to ensure only that security functions perform as specified.

AAL2 (Limited Authentication) is applicable in those circumstances where developers or users require a moderate level of independently assured security and are prepared to incur additional security-specific engineering costs. AAL2 requires the co-operation of the developer in terms of the delivery of design information and test results. AAL2 requires additional components from each of the Security Assurance Requirement classes except guidance documents. Authentication analysis is supported by the low-level design of the modules of the TOA, covert channel analysis and a subset of implementation of the TOA Security Functions. Development controls are supported by a life-cycle model, identification of tools, and partially automated configuration management.

AAL3 (Critical Authentication) is applicable where there is a need for higher level of independently assured security in a planned development, and a requirement for a rigorous development approach, without incurring unreasonable costs attributable to specialized security-engineering techniques. AAL3 is the preferred assurance level that any equipment used in a monitoring regime should have. AAL3 requires that the system be highly resistant to exploitation. A developer designed lifecycle model, the tracking of security flaws, and independent testing of a selected sample of developer tests enhances assurance.

AAL4 (Optimal Authentication) is the maximum level of assurance economically possible for equipment used in monitoring regimes. It is applicable where the value of the protected assets justifies the additional costs. AAL4 permits developers to gain a high level of assurance from the application of security engineering techniques to a rigorous development environment in order to produce a premium TOA for protecting high value assets against significant risks. AAL4 provides complete automation of configuration management, prevention of modification and compliance with implementation standards. Semi-formal responses from the developer are required for functional specifications, high-level design documentation and the TOA security policy model. The independent vulnerability assessments must ensure the system's resistance to external attacks. The developer must conduct a systematic search for covert channels, and test the low-level design. Development environment and configuration management controls are further strengthened.

CONCLUSIONS

Authentication is a necessary aspect of the implementation of systems for the assurance of compliance with non-proliferation and arms-control agreements. A consistent basis for this authentication activity has been developed by the United States technical community and is now being considered for monitoring systems being implemented in the Russian Federation.

The application of AALs allows a common language to be used in measuring the effectiveness of negotiated procedures with regard to monitoring equipment and facilities. The application of AALs allows for a degree of quantitative measurement of the effectiveness of authentication methods applied to monitoring equipment. The AALs can facilitate effective communication between the technical community and the policy community when discussing the requirements for systems and the consequences of negotiated procedures for authentication of monitoring equipment.

Authentication to a high level of confidence, such as AAL4 or greater, at reasonable cost is a desirable outcome for future nuclear non-proliferation activities in the FSU. Achieving this will require investments to support improvements in the quality of system development practice. These investments include support for standards development and adoption, and in training.

RECOMMENDATIONS

It is recommended that the DOE technical community further develop the AAL concept and definition for application to relevant monitoring regimes.

It is recommended that the DOE establish a bilateral Common Criteria Working Group involving an appropriate Russian Federation organization with goals of fostering adoption of the CC at the national level and establishing CC usage skills in selected organizations involved in non-proliferation and related activities.

Table 1. Examples of activities that may be included in achieving the AAL levels. These are given as exan represent the comprehensive set of activities performed to achieve that AAL.

	AAL 0 (~EAL 1 +EAL2)) Unauthenticated	**AAL1** (~EAL3) Minimally authenticated	**AAL2** (~EAL4) Limited authentication	**AAL3** (~EAL5) Critical authentication	au
Design Documentation	Design documentation **for commercial products** provided.	**Descriptive high-level design, configuration management,** and commercial product documentation provided, **participation in design reviews.**	**Descriptive low-level** design, configuration management, and commercial product documentation provided, participation in design reviews.	Complete system design, configuration management, **testing**, and commercial product documentation provided, **veto authority at design reviews.**	Comp design manag and co produ docum provid **partic** **desig**
Source Code Evaluation	**Incomplete** source code provided.	**All** source code provided.	All source code provided and a **line-by-line review of interesting areas of source code.**	All source code provided and an **exhaustive line-by-line review.**	All sou provid exhau line re **disass** **execu** **comp** **sourc**
Hardware Inspection	Comparison of hardware to **schematics and design documentation.**	**Random Selection and human** comparison of hardware **to previous photographs**.	Random selection and comparison of hardware **associated with a randomly selected subsystem** to previous photographs **using change detection software.**	Random selection and comparison of **all** hardware to previous photographs using change detection software.	Rando and co hardw photog chang softwa **metho** **identi** **comp**

BIBLIOGRAPHY

International Atomic Energy Agency (IAEA). (2001). *Working Document for IT Security Evaluation Criteria for Safeguards Equipment Systems*, Working Draft, Version 1.8, May 10, 2001, IAEA, Vienna, Austria.

International Organization for Standards (ISO). (1999). The Common Criteria for Information Technology Security Evaluation ISO-15408, August 1999, Version 2.1 Geneva, Switzerland.

Troy, Eugene F., (1998), *Common Criteria: Launching the International Standard*, NIST-ITL Bulletin,November 1998, (http://csrc.ncsl.nist.gov/cc/info/cc_bulletin.htm).

Geelhood, Bruce D.,(2001).Threat Statement Related to the Credibility of US-Specified Systems at FMSF Mayak, May 2001, Pacific Northwest National Laboratory, Richland, WA.

Geelhood, Bruce D., et al., (2001). *Design Guidelines for Authenticatable Systems*, PNNL-13386, Pacific Northwest National Laboratory, Richland, WA.

Kouzes, Richard T., et al. (2001a). *Authentication Procedures*, Authentication Task Force, PNNL-13550,May 2001, Pacific Northwest National Laboratory, Richland, WA.

Kouzes, Richard T., et al. 2001. *Authentication of Radiation Measurement Systems for Non-Proliferation*, PNNL-13386,May 2001, Pacific Northwest National Laboratory, Richland, WA.

International Security Community, (1997) *Common Evaluation Methodology for Information Technology Security, Part 1 - Introduction and general model*, Common Criteria Project, January 1997.

International Security Community, (1997) *Common Evaluation Methodology for Information Technology Security, Part 2* - Evaluation Methodology, Common Criteria Project, August 1999.

Software Engineering Institute, Carnegie Mellon University (2000a), Capability Maturity Model – *Integrated for Systems Engineering/Software Engineering/Integrated Product and Process Development* (CMMI-SE/SW/IPPD), *Staged Representation*, Version 1.02,, November 2000. Carnegie Mellon University, Pittsburgh PA.

Software Engineering Institute, Carnegie Mellon University (2000a), Capability Maturity Model – *Integrated for Systems Engineering/Software Engineering/Integrated Product and Process Development* (CMMI-SE/SW/IPPD), *Continuous Representation*, Version 1.02, November 2000, Carnegie Mellon University, Pittsburgh PA.

International Organization of Standards (ISO), (1995), *Information Technology, Standard for Software Life Cycle Processes* ISO/IEC 12207.

International Organization of Standards (ISO), (2000), *Information Technology - Life Cycle Management - System Life Cycle Processes*,2nd Committee Draft, ISO/IEC JTC1/SC7 N2257 January 2000.

Ambuel, Lynn, Michael McEvilley, *CC* Seminar, powerpoint presentationDecisive Analytics, , June 2001, Arlington VA.