# EVALUATION OF GRID SECURITY SOLUTIONS USING COMMON CRITERIA *

Syed Naqvi, Michel Riguidel, {naqvi, riguidel}@enst.fr
ENST – Télécom Paris, 46 rue Barrault, Paris 75013, France

## Abstract

*In the evolution of computational grids, security threats were overlooked in the desire to implement a high performance distributed computational system. But now the growing size and profile of the grid require comprehensive security solutions as they are critical to the success of the endeavor. A comprehensive security system, capable of responding to any attack on grid resources, is indispensable to guarantee its anticipated adoption by both the users and the resource providers. Some security teams have started working on establishing in-depth security solutions. The evaluation of their grid security solutions requires excellent criteria to assure sufficient security to meet the needs of its users and resource providers. Grid community's lack of experience in the exercise of the Common Criteria (CC), which was adopted in 1999 as an international standard for security product evaluation, makes it imperative that efforts be exerted to investigate the prospective influence of the CC in advancing the state of Grid security. This article highlights the contribution of the CC to establishing confidence in grid security, which is still in need of considerable attention from its designers. The process of security evaluation is outlined and the roles each part of the evaluation may play in obtaining confidence are examined.*

## 1. INTRODUCTION

The Common Criteria for Information Technology security evaluation is a relatively new program, which seeks to establish an internationally agreed-upon language for specifying security functionality, as well as an evaluation methodology to assess the strength of security implementations.

Grid computing may involve the sharing of critical data between systems in different organizations, security can be extremely important. As grid technology becomes more widely adopted by private industry, the need for security will increase even more. The complexity of Grid architecture makes it impossible to evaluate its security by *simple examination*. Moreover, for most users it is hardly possible to conduct more detailed checks, which are necessary for a qualified evaluation, as they can not afford the expenditure this would entail. The need to protect privacy and security of priceless data over the Grid is fueling even more need for common security evaluation criteria. Independent evaluation can be very useful for privacy enhancing technologies [1], as those very often aim at the protection of individual users, and this is exactly the user group that usually does not have enough resources to assess security on its own. These evaluation criteria have to be comprehensive, especially regarding privacy.

It is imperative for the Grid community to exercise some formal evaluation mechanism for the Grid security solutions. The prime objective of such assessment is to present a compelling case to already-skeptical potential Grid users and resource-providers in order to persuade them to participate in the global computing environment. The international recognition of the Common Criteria (CC) as security product evaluation standard, motivates us to explore its potential role in advancing the state of Grid Security.

This paper is organized in the following manner: An overview of the common criteria is given in section 2. A case study is presented in section 3 to demonstrate the use of common criteria for a Grid security solution. Based on this case study some discussion is made in section 4. Finally, some conclusions are drawn in section 5.

## 2. AN OVERVIEW OF COMMON CRITERIA (CC)

### 2.1. Historical Perspective

The first evaluation criteria arose out of the early work in the 1970s, and lead to the development of the renowned U.S. Trusted Computer Systems Evaluation Criteria (TCSEC) [2] between 1983 and 1985, more commonly referred to as the 'Orange Book'. Initial evaluation work was performed against the TCSEC, but quickly led to work within Europe to develop national criteria such as the UK Memorandum No. 3 [3], the Department of Trade and Industry Green Book [4] and the German [5] and French [6] criteria. Seeing the work going on in countries in Europe, earlier harmonization of the national evaluation criteria of France, Germany, the Netherlands and the UK resulted in the Information Technology Security Evaluation Criteria (ITSEC) [7].

* This research is supported by the European Commission funded project SEINIT (Security Expert Initiative) under reference number IST-2002-001929-SEINIT. The overall objective of the SEINIT project is to ensure a trusted security framework for ubiquitous environments, working across multiple devices and heterogeneous networks, in a way that is organization independent (inter-operable) and centered around an end-user. Project webpage is located at www.seinit.org

During this period, parallel activity in Canada led to the independent development of the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [8].

The U.S. recognized the need to replace the TCSEC, and in cooperation with Canada, began developing the Federal Criteria (FC). The draft FC was presented to the European Commission (EC) in early 1993. This led to a EC sponsored initiative to merge the draft FC with the ITSEC, resulting in the Common Criteria (CC) harmonization project. At this time there was parallel activity in the International Standards Organization (ISO), therefore a goal of the project was to feed back into the ISO forum to eventually have an international standard. CC was finally adopted in 1999 as an international standard for security product evaluation [9].

## 2.2. Objectives of the Common Criteria (CC)

A major criticism of the earlier criteria was that they were too defence or government focused, resulting in less interest from the commercial sector. Therefore the CC had the objective of addressing a wider marketplace extending beyond the immediate government sector into the commercial arena.

Earlier criteria, and the TCSEC in particular, had been criticized for being too fixed and unable to support a wider set of IT products or assurance. Therefore, the CC had the objective of being more flexible in its approach allowing more diverse products to be evaluated.

Finally, earlier criteria had been unable or slow to react to technological development and as a result had been blamed for stifling innovation. Therefore the CC had the objective of allowing the criteria to be extended in a controlled manner allowing growth with technology advances.

## 2.3. Evaluation Pattern

The first step of evaluating a system or application using common criteria methodology is to identify a Target of Evaluation (TOE.) The TOE is a system, application, or IT product that is selected to be evaluated according to CC standards. The second step is to develop a set of Security Targets (ST). The ST is the set of criteria to be applied for the evaluation of the TOE. For specific technologies or IT products, previously established protection profiles may be used as the ST criteria. With each step of the security framework, the CC evaluation process requires increasingly detailed information regarding the application or system security profile. Specific security mechanisms or techniques for IT products and technology are addressed through the Common Criteria Protection Profiles. The Common Criteria Evaluation and Validation Scheme Security Framework [10] is shown in figure 1.

There are three sections to the Common Criteria (CC) version 2.0. These three sections are Introduction and General Model (section one), Security Functional Requirements (section two), and Security Assurance Requirements (section three). The CC general audience, groups who would apply CC standards, is comprised of

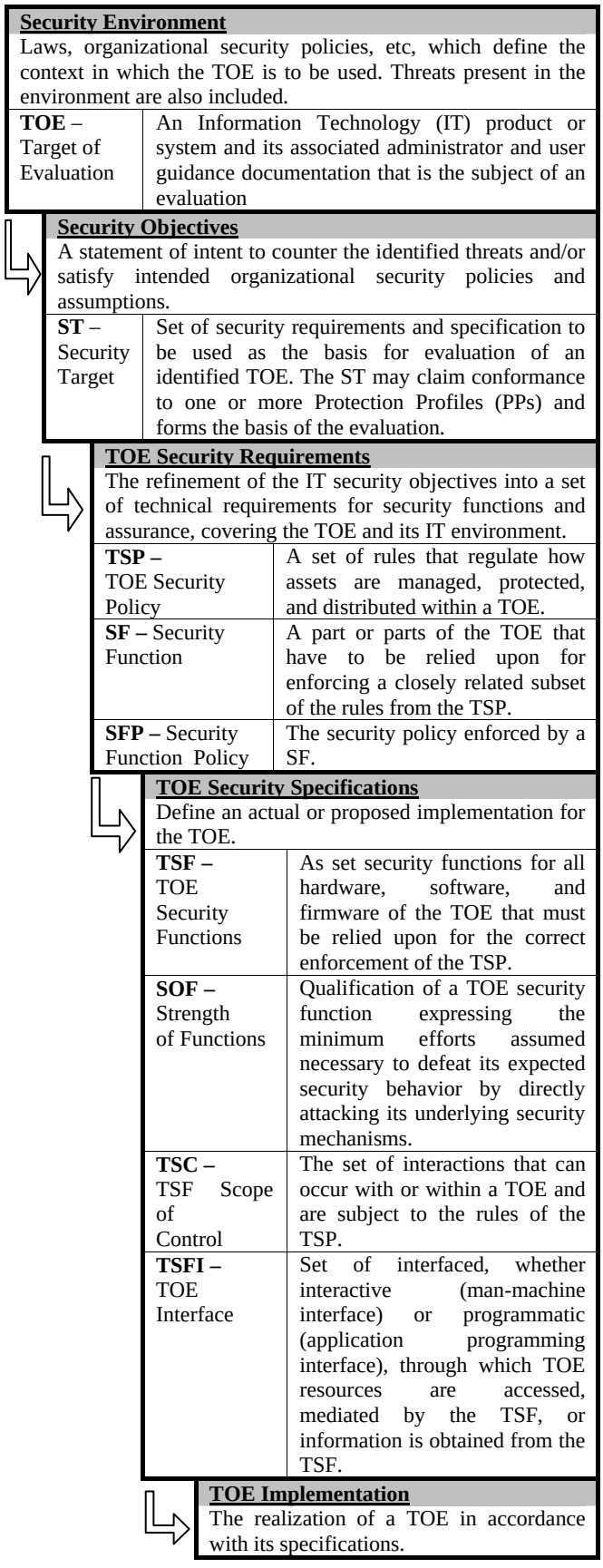


Figure 1: Common Criteria Evaluation and Validation Scheme Security Framework

IT system or product consumers, developers, and evaluators. The three CC sections provide guidance on how CC establishes baseline security requirements for buying, developing, or evaluating an IT system or product.

The technical specifications of applying IT security are provided in the second and third sections, security functional and assurance requirements, of the CC. These security requirements are grouped into high-level sets of related security requirements defined for the purposes of the CC as classes. The classes of related security requirements are unique to the either security functional requirements or security assurance requirements. Functional and assurance requirement classes guide consumers, developers, and evaluators on how to apply the security requirement components to meet security policy or counter threats.

## 3. A CASE STUDY

We present a case study of Health Grid to demonstrate how the common criteria is useful for the evaluation of Grid security solutions. First the Health Grid is briefly described, then its security properties are deduced using Common Criteria version 2.0.

### 3.1. Health Grid [11]

Health grids are Grid infrastructures comprising applications, services or middleware components that deal with the specific problems arising in the processing of medical data. Resources in health grids are databases, computing power, medical expertise and even medical devices. The vision of the health grid is to create an environment where information at the five levels (molecule, cell, tissue, individual, population) can be associated to provide individualized healthcare.

### 3.2. Security Architecture for Health Grid

Security is the most important issue. Personal data (any piece of information in which its owner can be identified, either directly or in combination with information that is available or can be available) is confidential, so access to the information must be performed only by authorized and authenticated persons, and data must be encrypted to guarantee its confidentiality and integrity. We have used our proposed security architecture for Health Grid [12] to produce protection profile.

### 3.3. Protection Profile for the Health Grid Security Architecture

A concise glimpse of the protection profile for the Health Grid is presented in this section.

**3.3.1. Protection Profile (PP):** The intent of this Protection Profile is to specify functional and assurance requirements applicable to Health Grid. Security requirements are viewed from the various angles including users, resource providers, and developers' views.

**3.3.2. Target of Evaluation (TOE):** This section describes the TOE as an aid to the understanding of its security requirements and address the product type, the intended usage and the general IT features of the TOE. The TOE is the *Health Grid*, independent of the application(s) being run over it.

**3.3.3. TOE Security Environment:** This section describes the security aspects of the environment in which the TOE is intended to be used and addresses the description of the assumptions, the threats and the organizational security policies.

**Assets** are security relevant elements of the TOE that are classified as: data and information across the TOE, applications running over the TOE, computing resources constituting the TOE, storage repositories of the TOE, communication links (wired and/or wireless) within the TOE.

**Assumptions** include a small community of active users (A.ActiveUsers), a large community of public users (A.PublicUsers), and a provision of periodic revision of the security architecture (A.TechnologyUpdates).

**Threats** are divided in the two broad categories: Threats to Information (T.I) and Threats to Resources (T.R).

**3.3.4. Security Objectives:** This section defines the security objectives for the TOE (O.T) and for its environment (O.E) with an emphasis on the use of state of art technologies to achieve these IT security objectives.

**3.3.5. TOE Security Requirements:** This section defines the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE.

**TOE Security Functional Requirements** define the functional requirements for the TOE using functional requirements components drawn from the Common Criteria part 2. The minimum strength of function (SOF) level for the TOE security requirements is *high* – SOF-high. SOF-high is a level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

**TOE Security Assurance Requirements** define the assurance requirements for the TOE using functional requirements components drawn from the Common Criteria part 3. The evaluation assurance level (EAL) is 4 – EAL4. EAL4 provides assurance by an analysis of the security functions, using a functional and complete interface specification, guidance documentation, the high-level and low-level design of the TOE, and a subset of the implementation, to understand the security behavior.

**3.3.6. Security Rationale:** This section presents the evidence used in the PP evaluation. This evidence

supports the claims that the PP is a complete and cohesive set of requirements and that TOE would provide an effective set of IT security countermeasures within the security environment. **Security Objectives Rationale** demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. **Security Requirements Rationale** demonstrates that the set of security requirements (TOE and environment) is suitable to meet and traceable to the security objectives.

## 4. DISCUSSION

The CC evaluation describes security problem and defines a set of security functions claimed to be able to solve the security problem effectively. The security functions defined in an evaluated ST with a pass verdict [13] can handle the security problem described in the same ST.

The CC evaluation of a security product is against an evaluated ST. A pass verdict of the CC evaluation assigned to a security product confirms that all assurance measures have been enforced effectively. As a result, a CC evaluated security product with a pass verdict is confirmed to have correctly implemented the security functions defined in the relevant ST, and hence can solve the identified security problem to some degree.

Here, it is exhibited that a security product may be capable of addressing certain security problem to some degree. It is this degree that is the critical metric for the measurement of confidence in security. This degree is determined by the security assurance measures enforced in the development activities. In order to ascertain in what aspects and to what extent that the security of a product is convincing, it is necessary to get acquaintance with the security assurance measures taken in the development of the product.

As mentioned in the beginning of the paper, Grid community lacks the experience of exercising Common Criteria. Within the reach of the authors' knowledge, there has not yet been discussion touching the topic in a similar way to that of the paper.

## 5. CONCLUSIONS

In order to capture the idea about what role the CC approach may play in setting up confidence in security of the Grid, we examined a case of Health Grid security architecture. It is imperative for the Grid community to get acquainted with the suitability and use of CC evaluation for the Grid security solutions. As it is said that security is a process, not a product and hence the security paradigms need regular review. Such reviews and consequent updates should be subject to vigorous evaluations. These evaluations can be facilitated by employing some internationally recognized evaluation standard like CC.

We are currently working on the virtualization of Grid security services. Our complete proposition is to be formalized to capture the whole range of security properties of Computational Grids. The ultimate goal of our research is to establish a formal Grid security model that could be used to earn confidence of Grid users and resource providers alike.

## 6. REFERENCES


[1] Tavani H., Moor J., *Privacy Protection, Control of Information, and Privacy-Enhancing Technologies*, ACM SIGCAS Computers and Society, volume 31, Issue 1, pp 6-11, March 2001, ISSN:00952737

[2] Department of Defense, Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, Washington DC, December 26, 1985

[3] UK Systems Security Confidence Levels, CESG Memorandum No. 3, Communications-Electronics Security Group, United Kingdom, January 1989

[4] DTI Commercial Computer Security Centre Evaluation Levels Manual, V22 Department of Trade and Industry, United Kingdom, February 1989

[5] Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems, ISBN 3887842006 German Information Security Agency (Bundesamt für Sicherheit in der Informationstechnik), Federal Republic of Germany, January 1989

[6] Catalogue de Critères Destinés à évaluer le Degré Confiance des Systèmes d'Information, 692/SGDN/DISSI/SCSSI Service Central de la Sécurité des Systèmes d'Information, July 1989

[7] Information Technology Security Evaluation Criteria, Version 1.2, Office for Official Publications of the European Communities, June 28, 1991

[8] The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) Version 3.0e. Canadian System Security Centre, Communications Security Establishment, Government of Canada, January 1993

[9] International Standards Organization, ISO/IEC 1508: Common Criteria, 1999

[10] Wallace K., *Common Criteria and Protection Profiles: How to Evaluate Information Technology Security*, SANS Institute GIAC practical repository – version 1.4b, 2003

[11] The Health Grid Organization, *Whitepaper on Health Grid*, 2004, http://www.healthgrid.org

[12] Naqvi S., Riguidel M., Demeure I., *Security Architecture for Health Grid using Ambient Intelligence*, Health Grid Conference 2004 (HG2004), Clermont-Ferrand, France, January 29-30, 2004

[13] Common Criteria Interpretation Management Board, *Common Criteria Evaluation Methodology for Information Technology Security, Part 2: Evaluation Methodology*, Version 1.0, CEM-99/045, Common Criteria Sponsoring Organizations, August 1999.