**IDEA GROUP PUBLISHING** **ITB12234**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
**edited by Merril Warkentin** © 2006, Idea Group Inc.

## Chapter XII

# High Assurance Products in IT Security

Rayford B. Vaughn, Mississippi State University, USA

## Abstract

*Corporate decisions concerning the purchase of security software and hardware appliances are often made based simply on the recommendations of the technical staff, the budget process (return on investment arguments), and/or a sales presentation and assertions. This chapter addresses the notion of trusted products and assurance in those products (i.e., confidence in the correct operation of a product) and how assurance is gained through independent review and testing. Early attempts to measure assurance in trusted products are described (some products today still refer to these procedures). Modern approaches to measuring assurance will be discussed in the context of ISO Standard 15408 (the* Common Criteria *(CC)). Current U.S. federal government policy concerning the use of evaluated products is presented, as well as a discussion of why industrial organizations may wish to consider such products.*

## Introduction

For a *chief information officer* (CIO), *chief security officer* (CSO), or *chief executive officer* (CEO) today, corporate oversight of *information technology* (IT) must involve significant interest in the area of computing security — to include the establishment of a robust defensive perimeter, the protection of corporate data assets (while stored, transmitted, and during processing), disaster recovery and response, and insuring that only authorized users access the system. These priorities are often offset by concerns

with return on investment, cost of data recovery, liability issues associated with misuse of system resources, and the business impact of security controls imposed on users of the system. In addition, those responsible for keeping intruders out of the systems under their care must often concern themselves with monitoring the activities of authorized users to insure proper "insider" behavior, compliance with mandated procedure, and to guard against damaging accidental destructive events. Executives faced with such responsibilities often rely on their technical staff to recommend architectures, system settings, procedures, and specific hardware/software products. This reliance, while appropriate in most circumstances, must be viewed with the understanding that there is today a critical shortage of computing security expertise and that system efficiency and ease of use objectives are very often adversely impacted by corporate security strategies and risk mitigation efforts. This chapter endeavors to offer a corporate IT decision maker some insights and suggestions that may be useful in selecting proper tools (hardware and software) and making the necessary investment in those tools. Subsequent chapters in this book will discuss specific tools and techniques needed by security engineers and the security engineering process itself.

The chapter begins with an overview of the notion of assurance in systems and what constitutes that assurance (informally defined as confidence that the product operates as intended). Some discussion of U.S. government guidelines and current policy is included here for the sake of historical completeness. Suggestions for how to select products are also provided in this chapter. The initial overview is followed by a more specific treatment of trusted products (a term often associated with high-assurance products). Since the mid-eighties, attempts have been made to measure the amount of assurance that one can place in the correct operation of a software product. This area is often loosely referred to as trusted products or assured system operation. An introduction is given to the current international standard for trusted systems (ISO Standard 15408 or Common Criteria), along with an overview of the older U.S. government *Trusted Computer System Evaluation Criteria* (or TCSEC). Both of these documents allow for a qualitative measurement of assurance in security software and/or hardware products. Following the discussion of trusted product measurement schemes, a brief explanation of how assurance measurement is assigned under the ISO Standard 15408 procedure is given. Several schemes of measurement exist today — the original *Department of Defense* (DOD) standard (sometimes referred to as the Orange Book rating), some residual European rating schemes, and today's ISO Standard 15408/CC measurements (i.e., Common Criteria *evaluation assurance levels* (EAL)). These rating schemes are later explained and defined. A high-level overview of the older TCSEC rating scheme will be briefly presented, followed by a more detailed discussion of how products are evaluated today and how the EAL level is determined (process-wise). The chapter concludes with a summary and some final thoughts for the reader.

# Overview

When one considers what products to purchase and to include in a security defensive perimeter, two high-level concerns should be addressed — the first is the completeness