**Chapter 22 Evaluating Systems**

* Evaluation assesses assurance evidence against functionality and assurance criteria, resulting in a trust measure reflecting how well a system meets specific criteria .
* The Trusted Computer System Evaluation Criteria (TCSEC) was the first formal evaluation methodology, with subsequent methodologies building and improving upon it .
* The Common Criteria (CC) is an internationally developed standard for security feature certification, and FIPS PUB 140-2 accredits cryptographic modules .

**22.1 Goals of Formal Evaluation**

* Perfect security is unachievable for complex computer systems; a trusted system meets specific security requirements under specific conditions .
* Evaluation methodologies define security functionality and assurance requirements, with a methodology to determine compliance and a trust level indicator .
* Formal evaluation methodologies provide trust measurements based on security requirements and assurance evidence, impacting development processes .

**22.1.1 Deciding to Evaluate**

* Formal evaluation decisions must balance security with costs like time and features, with vendors seeking validation due to government acquisition requirements .
* NSTISSP #11 mandates COTS products used on national security systems be evaluated against CC or FIPS 140-2 .
* Evaluation provides an independent assessment by experts, which can be used to compare products .

**22.1.2 Historical Perspective of Evaluation Methodologies**

* Government and military establishments were early drivers of computer security research and the creation of security evaluation processes .
* Evaluation methodologies provide functional requirements, assurance requirements, and levels of trust in different formats .
* The methodologies use slightly different terminologies .

**22.2 TCSEC: 1983-1999**

* TCSEC, or the Orange Book, was the first major computer security evaluation methodology, defining criteria for six evaluation classes (C1-A1) .
* The classes contain functional and assurance requirements, influenced by the reference monitor concept and Bell-LaPadula model .
* TCSEC emphasizes confidentiality and provides seven levels of trust measurement represented by the evaluation classes .

**22.2.1 TCSEC Requirements**

* TCSEC is organized by evaluation class, defining functional and assurance requirements within the context of the classes .
* Functional requirements include discretionary access control (DAC), object reuse, mandatory access control (MAC), and identification and authentication (I&A) .
* Assurance requirements include configuration management, trusted distribution, system architecture, design specification and verification, and testing .

**22.2.1.1 TCSEC Functional Requirements**

* Discretionary access control (DAC) requirements identify an access control mechanism that allows for controlled sharing of named objects by named individuals and/or groups .
* Mandatory access control (MAC) requirements, not required until class B1, embody the simple security condition and the \*-property from the Bell-LaPadula Model .
* Audit requirements address the existence of an audit mechanism as well as protection of the audit data .

**22.2.1.2 TCSEC Assurance Requirements**

* Configuration management requirements for the TCSEC begin at class B2 and increase for higher classes .
* Design specification and verification requirements address a large number of individual requirements, which vary dramatically among the evaluation classes .
* Testing requirements address conformance with claims, resistance to penetration, and correction of flaws followed by retesting .

**22.2.2 The TCSEC Evaluation Classes**

* Class C1, discretionary protection, has minimal functional requirements only for identification and authentication and for discretionary access controls .
* Class B1, labeled security protection, requires mandatory access controls, but these controls can be restricted to a specified set of objects .
* Class A1, verified protection, has the same functional requirements as class B3, but requires significant use of formal methods .

**22.2.3 The TCSEC Evaluation Process**

* Government-sponsored evaluators managed TCSEC evaluations, divided into application, preliminary technical review (PTR), and evaluation phases .
* The evaluation phase was divided into design analysis, test analysis, and a final review .
* The Ratings Maintenance Program (RAMP) maintained assurance for new versions of an evaluated product .

**22.2.4 Impacts**

* The TCSEC created a new approach to identifying how secure a product is, based on the analysis of design, implementation, documentation, and procedures .
* Its scope was limited .
* The evaluation process was difficult and often lacked needed resources .

**22.2.4.1 Scope Limitations**

* The TCSEC was written for operating systems and does not translate well to other types of products or to systems .
* The TCSEC focused on the security needs of the U.S. government and military establishments, who funded its development .
* Interpretations had limitations that restricted their utility .

**22.2.4.2 Process Limitations**

* The TCSEC evaluation methodology had two fundamental problems: "criteria creep" and evaluations took too much time .
* Vendors often had to do additional unanticipated work .
* Labs completing evaluations in roughly a year .

**22.2.4.3 Contributions**

* The TCSEC provided a process for security evaluation of commercial products .
* The TCSEC remained centered on operating systems, and its interpretations were insufficient to evaluate all types of networks or the new varieties of products .
* The commercial sector was dissatisfied with the functional requirements of the evaluation classes .

**22.3 International Efforts and the ITSEC: 1991-2001**

* By 1990, several Western countries had developed their own security evaluation criteria .
* The lack of reciprocity of evaluation among European nations created a move to harmonize the criteria of these countries, resulting in the Information Technology Security Evaluation Criteria (ITSEC), the European standard published in 1991 .
* ITSEC provided six levels of trust, called evaluation levels, E1, E2, E3, E4, E5, and E6 .

**22.3.1 ITSEC Assurance Requirements**

* The ITSEC assurance requirements were similar to those in the TCSEC, although there were substantial differences in terminology .
* The ITSEC required an assessment of the security measures used for the developer environment during the development and maintenance of the product or system .
* The effectiveness requirements of the ITSEC required several forms of vulnerability assessment that the TCSEC did not require .

**22.3.2 The ITSEC Evaluation Levels**

* The ITSEC levels were listed from lowest to highest .
* Level El required a security target against which to evaluate the product or system .
* Level E6 also required extensive use of formal methods .

**22.3.3 The ITSEC Evaluation Process**

* Each participating country had its own methodology for doing evaluations under the ITSEC .
* Vendors sought guidance and support from the consulting division to prepare for the evaluation, and con- sequently the products and systems were better prepared before evaluation began .
* The evaluation process was much more structured and did not have the lengthy (but technically sound) checks and balances that were provided by TCSEC technical review boards .

**22.3.4 Impacts**

* The ITSEC evaluation allowed flexibility in requirement definition and in mix- tures of assurance and functionality .
* In spite of the somewhat stronger assurance requirements in some areas, the ITSEC evaluations were often viewed as technically inferior to the TCSEC evaluations for two reasons .
* Another limit of the ITSEC was the lack of reciprocity of evaluation with Canada and the United States .

**22.3.4.1 Vendor-Provided Security Targets**

* Vendors did not always have qualified security experts to develop appropriate security targets .
* No official review provided checks and balances .
* The use of predefined functionality classes eased this limitation somewhat .

**22.3.4.2 Process Limitations**

* Some considered using the same company for both evaluation preparation support and evaluation itself to be a conflict of interest .
* Different personnel provided the consulting and evaluation services, but their biases could be the same .
* There was no body of experts to approve evaluator design analysis or to test coverage analysis .

**22.4 Commercial International Security Requirements: 1991**

* The Commercial International Security Requirements (CISR) was a joint effort of individuals from American Express and Electronic Data Systems (EDS) .
* The following discussion focuses on the differences between the requirements of the CISR and the TCSEC .
* Assurance requirements were identical to the TCSEC C2 requirements with one small addition .

**22.4.1 CISR Requirements**

* The CISR had its roots in the TCSEC evaluation class C2 .
* Assurance requirements were identical to the TCSEC C2 requirements with one small addition .
* The CISR added several new categories of requirements that were not found in the TCSEC .

**22.4.2 Impacts**

* Although the CISR never became a generally available evaluation methodology, it did contribute to the rapid growth of evaluation technology in the early 1990s .
* Perhaps the most significant contribution of this work was the awareness it brought to the U.Sfederal government regarding the security evaluation needs of the commercial sector .
* The CISR influenced the Federal Criteria, which included many of the new requirements stated by the CISR .

**22.5 Other Commercial Efforts: Early 1990s**

* In the late 1980s and early 1990s, private commercial companies in the United States and the United Kingdom began evaluating other types of products .
* This approach offered no level of trust but rather used a "pass-or-fail” process .
* They are still available today, but they must compete with the lowest level of trust Common Criteria evaluations that provide similar services at similar costs but provide a government-validated assurance rating .

**22.6 The Federal Criteria: 1992**

* The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) together developed the Federal Criteria (FC) in 1992 to replace the TCSEC with a new evaluation approach .
* A new direction in the FC is evaluation of products with respect to protection profiles, with each profile identifying requirements and other information particular to a family of products or systems .
* A protection profile (PP) is an abstract specification of the security aspects of an IT product .

**22.6.1 FC Requirements**

* The FC included a catalogue of all functional requirements of the TCSEC .
* Security management requirements were identified, enhanced, and added to a new section of the functional requirements .
* The FC included a new assurance requirement for a life cycle process .

**22.6.2 Impacts**

* The most significant contribution of the FC was the concept of an evaluated protection profile .
* The FC methodology supported evaluation of protection profiles .
* A second significant contribution was the development of a profile registry that made FC-approved protection profiles available for general use .

**22.7 FIPS 140: 1994-Present**

* During the time of the TCSEC, the U.S. government had no mechanism for evaluating cryptographic modules .
* In 1994, NIST and the Canadian Security Establishment (CSE) jointly established FIPS 140-1 as an evaluation standard for cryptographic modules for both countries .
* The Cryptographic Algorithm Validation Program (CAVP) provides for the evaluation of approved cryptographic algorithms against specific algorithm specifications .

**22.7.1 FIPS 140 Requirements**

* FIPS 140-1 and FIPS 140-2 provide the security requirements for a cryptographic module implemented within federal computer systems .
* Each standard defines four increasing, qualitative levels of security (called security levels) intended to cover a wide range of potential environments .
* The requirements for FIPS 140-2 include areas related to the secure design and implementation of cryptographic modules: specification; ports and interfaces; roles, services, and authentication .

**22.7.2 FIPS 140-2 Security Levels**

* Security Level 1 provides the lowest level of security .
* Security Level 3 requires enhanced physical security generally available in many existing commercial security products .
* Security Level 4 provides the highest level of security .

**22.7.3 Additional FIPS 140-2 Documentation**

* To promote consistency and repeatability, validation testing of cryptographic modules is performed using the Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules (DTR) .
* An Implementation Guidance for FIPS PUB 140-2, Security Requirements for Cryptographic Modules (IG) provides programmatic guidance of the CMVP .
* The content of the IG is based on responses provided by NIST and CSE to questions received from the FIPS 140-2 certification laboratories .

**22.7.4 Impact**

* The CMVP has improved the quality and security of cryptographic modules .
* Vendors were able to correct these problems before their modules and algorithms were deployed and used .
* In 2006, the first edition of ISO/IEC 19790 Information Technology Security Techniques — Security Requirements for Cryptographic Modules was published .

**22.7.5 Future**

* In 2005, NIST announced plans to develop FIPS 140-3, Security Requirements for Cryptographic Modules .
* FIPS 140-3 is currently in the internal review process .
* It will probably be released in the latter half of 2018 .

**22.8 The Common Criteria: 1998-Present**

* The Common Criteria (CC) approach to security evaluation draws from the strengths of TCSEC, ITSEC, CTCPEC, and FC, as well as from commer- cial efforts .
* The Common Criteria evaluation methodology has three parts: the CC documents, the CC Evaluation Methodology (CEM), and a country-specific evaluation methodology called an Evaluation Scheme or National Scheme .
* There have been many versions of the CC and its companion CC Evalua- tion Methodology (CEM) .

**22.8.1 Overview of the Methodology**

* The CC supports two kinds of evaluations: evaluations of protection profiles and evaluations of products or systems against security targets (STs) .
* The concept of a protection profile evolved from the Federal Criteria, the CTCPEC profiles, and the ITSEC functionality classes .
* The second form of evaluation offered by the CC is the evaluation of a product or system against a security target (ST) .

**22.8.2 CC Requirements**

* The heart of the CC is the requirements themselves .
* The CC defines both functional and assurance requirements and then builds EALs out of the assurance requirements .
* Functional and assurance requirements are divided into classes based on common purpose .

**22.8.3 CC Security Functional Requirements**

* There are 11 classes of security functional requirements, each having one or more families .
* Requirements may be hierarchical in nature .
* All other requirements are derived from previously discussed methodologies .

**22.8.4 Assurance Requirements**

* There are nine security assurance classes .
* One assurance class relates to protection profiles, one to security targets, and one to the maintenance of assurance .
* The other six directly address assurance for the product or system .

**22.8.5 Evaluation Assurance Levels**

* The CC has seven levels of assurance .
* EAL1: Functionally Tested .
* Figure 22-1 gives a rough matching of the levels of trust of various methodologies .

**22.8.6 Evaluation Process**

* The CC evaluation process in the United States is controlled by the CC Evaluation Methodology (CEM) and NIST .
* Evaluations are performed by NIST-accredited commercial laboratories that do evaluations for a fee .
* Typically, a vendor selects an accredited laboratory to evaluate a product or system .

**22.8.7 Other International Organizations**

* Over the years, a few additional entities have been created as a result of the CC .
* Two of these are described in this section .
* The Senior Officials Group Information Systems Security (SOG-IS) agreement is a mutual recognition agreement between participating government organizations and agencies from countries in the European Union (EU) or European Free Trade Association (EFTA) .

**22.8.7.1 SOG-IS International Cooperation Agreement**

* The Senior Officials Group Information Systems Security (SOG-IS) agreement is a mutual recognition agreement between participating government organizations and agencies from countries in the European Union (EU) or European Free Trade Association (EFTA) .
* SOG-IS participants collaborate to standardize CC PPs and CC certificate policies between the CC schemes within Europe to present a common position within the CCRA and to develop PPs when the EU Commission issues an IT security-related directive that should be incorporated in EU national laws .
* There are currently two techni- cal areas covered by the SOG-IS agreement: smartcards and similar devices, and hardware devices with security boxes .

**22.8.7.2 Common Criteria Users Forum**

* The Common Criteria Users Forum is comprised of international individual members from the following sectors: academia, consultants, end users, govern- ments, CC laboratories, schemes, solution providers, standards organizations, and vendors .
* The CCUF provides a communication mechanism between individuals in the CC community .
* The CCUF is governed by the CCUF Management board, which is com- prised of seven elected members .

**22.8.8 Impacts**

* The CC addresses many issues with which other evaluation criteria and method- ologies have struggled .
* In some sense, this is true .
* The CC is much more complete than the functional requirements of most preceding technologies .

**22.8.9 Future of the Common Criteria**

* The CC documentation and methodology continue to evolve .
* New Technical Communities are continuing to be formed and cPPs are continuing to be developed by these new TCs .
* The Common Criteria Management Board (CCMB) is an international body responsible for maintaining the Common Criteria and ensuring the CCRA is operated as defined by its rules .

**22.9 SSE-CMM: 1997-Present**

* The System Security Engineering Capability Maturity Model (SSE-CMM) is a process-oriented methodology for developing secure systems based on the Software Engineering Capability Maturity Model (SE-CMM) .
* Capability models define requirements for processes, whereas methodologies such as the CC and its predecessors define requirements for secu- rity functionality .
* Applying the SSE-CMM can support assurance evidence and increase confidence in the trustworthiness of a product or system .

**22.9.1 The SSE-CMM Model**

* The SSE-CMM is organized into processes and maturity levels .
* Generally speaking, the processes define what needs to be accomplished by the security engineering process and the maturity levels categorize how well the process accomplishes its goals .
* The SSE-CMM contains 11 systems security engineering process areas .

**22.9.2 Using the SSE-CMM**

* Application of the SSE-CMM is a straightforward analysis of existing processes to determine which base processes have been met and the maturity levels they have achieved .
* This is accomplished using the well-defined base processes and Capability Maturity Levels that were overviewed in the preceding section .
* A useful way of looking at the result of a complete SSE-CMM analysis is to use a Rating Profile, which is a tabular representation of process areas versus maturity levels .

**22.10 Summary**

* Since the early 1980s, the international computer security community has been developing criteria and methodologies for the security evaluation of IT products and systems .
* New methodologies were developed to address these issues .
* These foundational methodologies have culminated in the Common Criteria, which has obtained worldwide support for over a decade .

**22.11 Research Issues**

* The Common Criteria (CC) methodology is the focus of much current research .
* Evaluations are expensive and time-consuming .
* Consumers of products and systems need to determine how effective those products and systems are in their current environments .

**22.12 Further Reading**

* The evaluation process of the TCSEC has been widely discussed and critiqued .
* The basis for CC requirements arises in several papers, including one that describes the functional criteria for distributed systems .
* The most current information on evaluation standards and processes can be found on the World Wide Web .