Standardization and Security Criteria: Security Evaluation of Computer Products 16

16.1 Introduction

The rapid growth of information technology (IT), our growing dependence on it, and the corresponding skyrocketing security problems arising from it have all created a high demand for comprehensive security mechanisms, and best practices mitigate these security problems. Solutions on two fronts are sought for. First well-implemented mechanisms and best practices are needed for fundamental security issues like cryptography, authentication, access control, and audit. Second, comprehensive security mechanisms are also needed for all security products so that consumers are assured of products and systems that meet their business security needs. The response to this high demand for security products has been an avalanche of products of all types, capabilities, varying price range, effectiveness, and quality. You name a product and you get a flood from vendors. As the marketplace for security products get saturated, competing product vendors and manufacturers started making all sorts of claims about their products in order to gain a market niche. In this kind of environment then, how can a customer shop for the right secure product, what security measures should be used, and how does one evaluate the security claims made by the vendors? Along the way, making a choice of a good effective security product for your system or business has become a new security problem we want to focus on in this chapter.

Buying computer products, even without the thousands of overzerous vendors and manufacturers fighting to make a buck, has never been easy because of the complexity of computer products to the ordinary person. One cannot always rely on the words of the manufacturers and those of the product vendors to ascertain the suitability and reliability of the products. This is currently the case in both computer hardware and software products. It is a new computer security problem all computer product buyers must grapple with and computer network managers must try to mitigate as they acquire new computer products.

There are several approaches to deal with this new security problem, but we will discuss two here: standardization and security evaluation of products. Since

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_16

standardization leads into security evaluation, meaning that product security evaluation is done based on established standards, we will start with standardization.

16.2 Product Standardization

A standard is a document that establishes uniform engineering or technical specifications, criteria, methods, processes, or practices. Some standards are mandatory, while others are voluntary [1]. Standardization is then *a process* of agreeing on these standards. The process itself is governed by a Steering Committee that consists of representatives from the different engineering and technical areas with interests in the product whose standard is sought. The committee is responsible for drafting the standard legal and technical document, from product specifications, establishing processes by which the draft standards are reviewed and accepted by the interested community.

Theoretically, the process itself sounds easy and consists of several stages through which the product specifications must undergo. First, the specifications undergo a period of development and several iterations of review by the interested engineering or technical community, and the revisions are made based on members' experiences. These revisions are then adopted by the Steering Committee as draft standards. But as Bradner [2] observes, in practice, the process is more complicated, due to (1) the difficulty of creating specifications of high technical quality, (2) the need to consider the interests of all of the affected parties, (3) the importance of establishing widespread community consensus, and (4) the difficulty of evaluating the utility of a particular specification for the community.

In any case, the goals of this process are to create standards that [2]:

- Are technically excellent.
- Have prior implementation and testing.
- Are clear, concise, and easily understood documentation.
- Foster openness and fairness.

16.2.1 Need for Standardization of (Security) Products

Whenever a product is designed to be used by or on another product, the interfaces of the two products must agree to meet and talk to each other every time these two products are connected to each other. What this is saying is that *interface specification* is the protocol language these two products talk, enabling them to understand each other. If there are conflicts in the specification language, the two will never understand each other, and they will never communicate.

Products and indeed computer products are produced by many different companies with varying technical and financial capabilities based on different technical design philosophies. But however varied the product marketplace may be, the interface specifications for products meant to interconnect must be compatible.

Standardization reduces the conflicts in the interface specifications. In other words, standardization is needed to enforce conformity in the product interface specifications for those products that are meant to interconnect.

According to Rebecca T. Mercuri [3], standards provide a neutral ground in which methodologies are established that advance the interest of manufacturers as well as consumers while providing assurances of safety and reliability of the products. Currently, the computer industry has a large variety of standards covering every aspect of the industry.

Standards are used in setting up of product security testing procedures, the passing of which results in a certification of the product. However, as Mercuri notes, certification alone does not guarantee security. There are cases where it is only a sign of compliance. Because of this and other reasons, many of the major product security testing bodies and governments have a collection of standards that best test the security of a product. These standards are called *criteria*. Many of the criteria we are going to look at have several tiers or levels where each level is supposed to certify one or more requirements by the product.

16.2.2 Common Computer Product Standards

The rapid growth of computer technology has resulted into a mushrooming of standards organizations that have created thousands of computer-related standards for the certification of the thousands of computer products manufactured by hundreds of different manufacturers. Among the many standards organizations that developed the most common standards used by the computer industry today are shown in Table 16.1 [4].

16.3 Security Evaluations

Security evaluation of computer products by independent and impartial bodies creates and provides security assurance to the customers of the product. The job of the security evaluators is to provide an accurate assessment of the strength of the security mechanisms in the product and systems based upon a criterion [5]. Based on these evaluations, an acceptable level of confidence in the product or system is established for the customer.

The process of product security evaluation for certification consists of two components: the *criteria* against which the evaluations are performed and the *schemes* or methodologies which govern how and who can perform such security evaluations [5]. There are several criteria and methods used internationally, and we are going to discuss some in the following sections. The process of security evaluation, based on criteria, consists of a series of tests based on a set of levels where each level may test for a specific set of standards. The process itself starts by establishing the following [1]:

Table 16.1 Computer products and system-related standards organizations

Standards organization	Standards developed
American National Standards Institute (ANSI)	Has a lot of American and international standards. See http://webstore.ansi.org/sdo.aspx
British Standards Institute (BSI)	BS XXX: Year Title where XXX is the number of the standard (many)
Institute of Electrical and Electronic Engineers Standards Association (IEEE-SA)	Has thousands of standards. See http://www.ieee.org/web/publications/subscriptions/prod/standards_overview.html
International Organization for Standardization (ISO)	Has developed over 17,000 international standards on a variety of subjects with about 1100 new ISO standards that are published every year. http://www.iso.org/iso/iso_catalogue.htm
National Institute of Standards and Technology (NIST)	Supports over 1300 different Standards. See http://ts.nist.gov/MeasurementServices/ReferenceMaterials/PROGRAM_INFO.cfm
Organization for the Advancement of Structured Information Standards (OASIS)	Has a long list of standards. See http://www.oasisopen.org/specs/index.php
Underwriters Laboratories (UL)	Has developed more than 1000 standards for safety. See http://www.ul.com/info/standard.htm
World Wide Web Consortium (W3C)	W3C creates primarily Web standards and guidelines designed to ensure long-term growth for the Web. See http://www.w3.org/

- Purpose
- Criteria
- Structure/elements
- Outcome/benefit

16.3.1 Purpose of Security Evaluation

Based on the Orange Book, a security assessment of a computer product is done for [1]:

- Certification—To certify that a given product meets the stated security criteria and therefore is suitable for a stated application. Currently, there is a variety of security certifying bodies of various computer products. This independent evaluation provides the buyer of the product added confidence in the product.
- Accreditation—To decide whether a given computer product, usually certified, meets stated criteria for and is suitable to be used in a given application. Again, there are currently several firms that offer accreditations to students after they use and get examined for their proficiency in the use of a certified product.
- Evaluation—To assess whether the product meets the security requirements and criteria for the stated security properties as claimed.

Table 16.2 Common computer security products' standards

B	**I**
Blacker (security)	IEC 60870-6
BS 7799	IEEE 802.10
C	ISO 15292
Common Criteria	ISO/IEC 27002
Content Security Policy	ITSEC
CTCPEC	**N**
CVSS	NIST Cybersecurity Framework
Cyber Resilience Review	**P**
Cybersecurity standards	Pluggable authentication module
F	**R**
FIPS 140	Rainbow Series
FIPS 140-2	**S**
FIPS 140-3	S/MIME
FIPS 199	Security Content Automation Protocol
H	Standard of Good Practice
HTTP Strict Transport Security	**T**
	Trusted Computer System Evaluation Criteria

Source: Wikipedia. https://en.wikipedia.org/wiki/Category:Computer_security_standards

- Potential market benefit, if any for the product. If the product passes the certification, it may have a big market potential.

16.3.2 Security Evaluation Criteria

As we have discussed earlier, *security evaluation criteria* are a collection of security standards that define several degrees of rigor acceptable at each testing level of security in the certification of a computer product. The security of most computer products is evaluated based on the security standards in Table 16.2.

Security evaluation criteria also may define the formal requirements the product needs to meet at each assurance level. Each security evaluation criterion consists of several assurance levels with specific security categories in each level. See the Orange Book (TCSEC) criteria assurance levels in Sect. 16.3.3.

Before any product evaluation is done, the product evaluator must state the evaluation criteria to be used in the process in order to produce the desired result. By stating the evaluation criteria, the evaluator directly states the assurance levels and categories in each assurance level that the product must meet. The result of a product evaluation is the statement whether the product under review meets the stated assurance levels in each evaluation criteria category. The Trusted Computer System Evaluation Criteria widely used today all have their origin in and their assurance levels based on the Trusted Computer System Evaluation Criteria (TCSEC) in Sect. 16.3.3.

16.3.3 Basic Elements of an Evaluation

The structure of an effective evaluation process, whether product oriented or process oriented, must consider the following basic elements:

- *Functionality*: Because acceptance of a computer security product depends on what and how much it can do. If the product has limited utility and in fact if it does not have the needed functionalities, then it is of no value. So the number of functionalities the product has or can perform enhances the product's acceptability.
- *Effectiveness*: After assuring that the product has enough functionalities to meet the needs of the buyer, the next key question is always whether the product meets the effectiveness threshold set by the buyer in all functionality areas. If the product has all the needed functionalities, but these functionalities are not effective enough, then the product cannot guarantee the needed security, and therefore, the product is of no value to the buyer.
- *Assurance*: To give the buyer enough confidence in the product, the buyer must be given an assurance, a guarantee, that the product will meet nearly all, if not exceed, the minimum stated security requirements. Short of this kind of assurance, the product may not be of much value to the buyer.

16.3.4 Outcome/Benefits

The goal of any product producer and security evaluator is to have a product that gives the buyer the best outcome and benefits within a chosen standard or criteria. The product outcome may not come within a short time, but it is essential that eventually the buyers see the security benefits. Although the process to the outcome for both the evaluator and the buyer may be different, the goal must always be the same, a great product. For example, to the product evaluator, it is important to minimize the expenses on the evaluation process without cutting the stated value of the evaluation. That is to say that keeping costs down should not produce mediocre outcomes. However, to the buyer, the process of evaluation of a software product for security requirements must ultimately result in the best product ever in enhancing the security of the system where the product is going to be deployed. The process of evaluation is worth the money if the product resulting from it meets all buyer requirements and better if it exceeds them.

The evaluation process itself can be done using either a standard or criteria. The choice of what to use is usually determined by the size of the product. Mostly, small products are evaluated using standards, while big ones are evaluated using criteria. For example, a computer mouse I am using is evaluated and certified by the standards developed by the Underwriters Laboratories, Inc., and the mouse has an insignia UL in a circle. If you check your computer, you may notice that each component is probably certified by a different standard.

Let us now look at the evaluation process itself. The evaluation of a product can take one of the following directions [1]:

- Product oriented: This is an investigative process to thoroughly examine and test every state security criteria and determine to what extent the product meets these stated criteria in a variety of situations. Because covering all testable configurations may require an exhaustive testing of the product, which is unthinkable in software testing, for example, a variety of representative testing must be chosen. This, however, indicates that the testing of software products, especially in security, depends heavily on the situation the software product is deployed in. One has to pay special attention to the various topologies in which the product is tested in and whether those topologies are exhaustive enough for the product to be acceptable.
- Process oriented: This is an audit process that assesses the developmental process of the product and the documentation done along the way, looking for security loopholes and other security vulnerabilities. The goal is to assess how a product was developed without any reference to the product itself. Unlike product-oriented testing which tends to be very expensive and time-consuming, process-oriented testing is cheap and takes less time. However, it may not be the best approach in security testing because its outcomes are not very valuable and reliable. One has to evaluate each evaluation scheme on its own merit.

Whatever direction of evaluation is chosen, the product security evaluation processes can take the following steps [1]:

- *Proposal review*: Where the product is submitted by the vendor for consideration for a review. The market analysis of the product is performed by the evaluator [in the United States, it is usually the Trusted Product Evaluation Program (TREP) within the National Security Agency (NSA)] based on this proposal.
- *Technical assessment*: After the initial assessment, the product goes into the technical assessment (TA) stage where the design of the product is put under review. Documentation from the vendor is important at this stage.
- *Advice*: From the preliminary technical review, advise is provided to the vendor to aid the vendor in producing a product and supporting documentation that is capable of being evaluated against a chosen criterion.
- *Intensive preliminary technical review*: An independent assessment by the evaluator to determine if the product is ready for evaluation. This stage can be done as the vendor's site and evaluators become familiar with the product.
- *Evaluation* is a comprehensive technical analysis of every aspect of the product. Rigorous testing of every component of the product is done. At the end, if the product passes all the tests, it is awarded an Evaluated Products List (EPL) entry.
- *Rating maintenance phase* provides a mechanism for the vendor to maintain the criteria rating of the product. If security changes are needed to be made, the vendor makes them during this phase. At the end of the phase, a full approval of the product is recommended. The rating is then assigned to the product.

16.4 Major Security Evaluation Criteria

The best way product manufacturers and vendors can demonstrate to their customers the high level of security their products have is through a security evaluation criteria. Through security evaluation, independent but accredited organizations can provide assurance to product customers of the security of product. These evaluations, based on specified criteria, serve to establish an acceptable level of confidence for product customers. Consequently, there are two important components of product security evaluations: the *criteria* against which the evaluations are performed and the *schemes* or methodologies which govern how and by whom such evaluations can be officially performed [6].

There are now several broadly accepted security evaluation criteria to choose from. However, this is a recent phenomenon. Before that, there were small national criteria without widely used and accepted standard criteria. Every European country and the United States each had its own small criteria. But by the mid-1980s, the European countries abandoned their individual national criteria to form the combined Information Technology Security Evaluation Criteria (ITSEC) (see Sect. 16.3.4) to join the US TCSEC that had been in use since the 1960s. Following the merger, an international criteria board finally introduced a widely accepted International Organization for Standardization (ISO)-based Common Criteria (CC). Let us look at a number of these criteria over time.

16.4.1 Common Criteria (CC)

The Common Criteria (CC) is a joint effort between nations to develop a single framework of mutually recognized evaluation criteria. It is referred to as the Harmonized Criteria, a multinational successor to the TCSEC and ITSEC that combined the best aspects of ITSEC, TCSEC, CTCPEC (Canadian Criteria), and the US Federal Criteria (FC). It was internationally accepted and finalized as an ISO 15408 standard and has been embraced by most countries around the world as the de facto security evaluation criteria. Common Criteria version 2.3 (CC v2.3) consists of three parts:

- Introduction and general model
- Security functional requirements
- Security assurance requirements

Based on these parts, CC v2.3 awards successfully evaluated products' one of eight evaluation assurance level (EAL) ratings from EAL 0 (lowest) to EAL7 (highest). For more information on CC v2.3, see http://www.commoncriteriaportal.org/thecc.html.

16.4.2 FIPS

Information technology (IT) product manufacturers always claim that their products offer the desired security for whatever purpose. This claim is difficult to prove especially for smaller businesses. IT customers, including the government, in need of protecting sensitive data need to have a minimum level of assurance that a product will attain a certain level of required security. In addition to this, legislative restrictions may require certain types of technology, such as cryptography and access control, to be in all products used by either government or specific businesses. In this case, therefore, those products need to be tested and validated before they are acquired.

Under needs like these, the Information Technology Management Reform Act (Public Law 104–106) requires that the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for federal computer systems. NIST's standards and guidelines are issued as Federal Information Processing Standards (FIPS) for government-wide use. NIST develops FIPS when there are compelling federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

Under these standards and guidelines, products are validated against FIPS at ranging security levels from the lowest to the highest. The testing and validation of products against the FIPS criteria may be performed by NIST and CSE-approved and accredited certification laboratories. Level 2 is the highest level of validation pursued by software vendors, while level 4 is generally only attempted by hardware vendors. For more information, see http://www.itl.nist.gov/fipspubs/.

16.4.3 The Orange Book/TCSEC

Most of the security criteria and standards in product security evaluation have their basis in the *Trusted Computer System Evaluation Criteria* (TCSEC), the first collection of standards used to grade or rate the security of computer system products. The TCSEC has come to be a standard commonly referred to as "the Orange Book" because of its orange cover. The criteria were developed with three objectives in mind [7]:

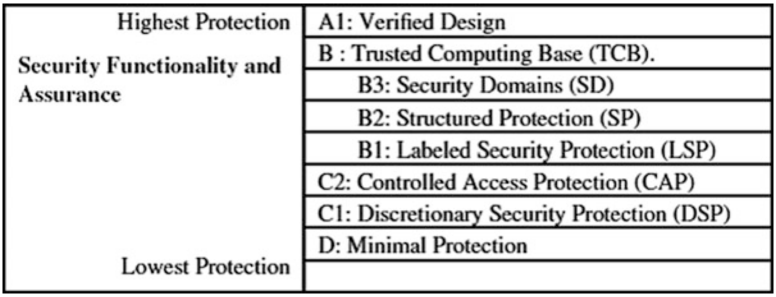
- To provide users with a yardstick with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information
- To provide guidance to manufacturers as to what to build into their new, widely available trusted commercial products in order to satisfy trust requirements for sensitive applications
- To provide a basis for specifying security requirements in acquisition specifications

The criteria also address two types of requirements:

- Specific security feature requirements
- Assurance requirements

The criteria met these objectives and requirements through four broad hierarchical divisions of enhanced assurance levels. These divisions, as seen in Fig. 16.1, labeled D for minimum protect, C for discretionary protection or need-to-know protection, B for mandatory protection, and A for verified protection are detailed as follows [1, 7]:

- *Class D (Minimal Protection)*: A division containing one class reserved for systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.
- *Class C*:
  - *C1 (Discretionary Security Protection (DSP))***:** This is intended for systems in environments where cooperating users process data at the same level of integrity. Discretionary access control (DAC) based on individual users or groups of users enabled them to securely share access to objects between users and groups of users after user identification and authentication. This makes it impossible for other users from accidentally getting access to unauthorized data.
  - *C2: Controlled Access Protection (CAP)* is a system that makes users accountable for their actions. DAC is enforced at a higher granularity level than C1. Subjects with information of another subject must not get access rights to an object which makes users accountable for their actions through log-in and auditing procedures.
- *Class B*: The notion of a security-relevant portion of a system is called a Trusted Computing Base (TCB). A TCB that preserves the integrity of the sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division:
  - *B1 (Labeled Security Protection (LSP))*: This is intended for systems dealing with classified data. Each system has all the requirements in C2 and in addition has an informal requirement of the security policy model, data labels for subjects and objects whose integrity must be strictly guarded, and mandatory access control over all subjects and objects.
  - *B2 (Structured Protection (SP))*: To add security requirements to the design of the system, thus increasing security assurance. It also requires the TCB to be based on a security policy. The TCB interface must be well defined to be subjected to a more thorough testing and complete review. In addition, it strengthens authentication mechanism, trusted facility management provided, and configuration management imposed. Overall systems with B2 certification are supposed to be resistant to penetration.
  - *B3 (Security Domains (SD))*: To ensure a high resistance to penetration of systems. It requires a security administrator and an auditing mechanism to



Highest Protection	A1: Verified Design
Security Functionality and Assurance	B : Trusted Computing Base (TCB).
	B3: Security Domains (SD)
	B2: Structured Protection (SP)
	B1: Labeled Security Protection (LSP)
	C2: Controlled Access Protection (CAP)
	C1: Discretionary Security Protection (DSP)
	D: Minimal Protection
Lowest Protection	

Fig. 16.1 The TCSEC/Orange Book class levels

monitor the occurrence or accumulation of security-relevant events. Such events must always trigger an automatic warning. In addition, a trusted recovery must be in place.

Class A1 (Verified Protection) This division is characterized by the use of formal security verification methods to ensure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development, and implementation.

Most evaluating programs in use today still use or refer to TCSEC. Among these programs are [3]:

- The Trusted Product Evaluation Program (TPEP). TPEP is a program with which the US Department of Defense's National Computer Security Center (NCSC) evaluates computer systems.
- The Trust Technology Assessment Program (TTAP). TTAP is a joint program of the US National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). TTAP evaluates off-the-shelf products. It establishes, accredits, and oversees commercial evaluation laboratories focusing on products with features and assurances characterized by TCSEC B1 and lower level of trust (see Sect. 15.3.1 for details).
- The Rating Maintenance Phase (RAMP) Program was established to provide a mechanism to extend the previous TCSEC rating to a new version of a previously evaluated computer system product. RAMP seeks to reduce evaluation time and effort required to maintain a rating by using the personnel involved in the maintenance of the product to manage the change process and perform security analysis. Thus, the burden of proof for RAMP efforts lies with those responsible for system maintenance (i.e., the vendor or TEF) other than with an evaluation team.

- The Trusted Network Interpretation (TNI) of the TCSEC, also referred to as "The Red Book," is a restating of the requirements of the TCSEC in a network context.
- The Trusted Database Interpretation (TDI) of the TCSEC is similar to the Trusted Network Interpretation (TNI) in that it decomposes a system into smaller independent parts that can be easily evaluated. It differs from the TNI in that the paradigm for this decomposition is the evaluation of an application running on an already evaluated system. The reader is also referred to <http://www.radium. ncsc.mil/tpep/library/rainbow/5200.28-STD.html#HDR4> for an extensive coverage of the standard criteria.

16.4.4 Information Technology Security Evaluation Criteria (ITSEC)

While the US Orange Book criteria were developed in 1967, the Europeans did not define unified valuation criteria well until the 1980s when the United Kingdom, Germany, France, and the Netherlands harmonized their national criteria into a European Information Technology Security Evaluation Criteria (ITSEC). Since then, they have been updated, and the current issue is version 1.2, published in 1991, followed 2 years later by its user manual, the IT Security Evaluation Manual (ITSEM), which specifies the methodology to be followed when carrying out ITSEC evaluations. ITSEC was developed because the Europeans thought that the Orange Book was too rigid. ITSEC was meant to provide a framework for security evaluations that would lead to accommodate new future security requirements. It puts much more emphasis on integrity and availability. For more information on ITSEC, see http://www.radium.ncsc.mil/tpep/library/non-US/ITSEC-12.html.

16.4.5 The Trusted Network Interpretation (TNI): The Red Book

The Trusted Network Interpretation (TNI) of the TCSEC, also referred to as "The Red Book," is a restating of the requirements of the TCSEC in a network context. It attempted to address network security issues. It is seen by many as a link between the Red Book and new criteria that came after. Some of the shortfalls of the Orange Book that the Red Book tries to address include the distinction between two types of computer networks [7]:

- Networks of independent components with different jurisdictions and management policies
- Centralized networks with single accreditation authority and policy

While the Orange Book addresses only the first type, the second type presents many security problems that the Red Book tries to address. Including the evaluations of network systems, distributed or homogeneous, often made directly against the

TCSEC without reference to the TNI. TNI component ratings specify the evaluated class as well as which of the four basic security services the evaluated component provides. Read more about these difference in the paper "Network Security: Red Book vs. Orange Book Evaluation," by Rich Lee at https://support.novell.com/techcenter/tips/ant19960603.html.

16.5 Does Evaluation Mean Security?

As we noted in Sect. 16.4, the security evaluation of a product based on a criterion does not mean that the product is assured of security. No security evaluation of any product can guarantee such security. However, an evaluated product can demonstrate certain security mechanisms and features based on the security criteria used and demonstrate assurances that the product does have certain security parameters to counter many of the threats listed under the criteria.

The development of new security standards and criteria will no doubt continue to result in better ways of security evaluations and certification of computer products and will therefore enhance the computer systems' security. However, as Mercuri observes, product certification should not create a false sense of security.

Exercises

1. The US Federal Criteria drafted in the early 1990s were never approved. Study the criteria and give reasons why they were not developed.
2. One advantage of process-oriented security evaluation is that it is cheap. Find other reasons why it is popular. Why, despite its popularity, is it not reliable?
3. For small computer product buyers, it is not easy to apply and use these standard criteria. Study the criteria and suggest reasons why this is so.
4. Nearly all criteria were publicly developed; suggest reasons why? Is it possible for individuals to develop commercially accepted criteria?
5. There are evaluated computer products on the market. Find out how one finds out whether a computer product has a security evaluation.
6. If you have a computer product, how do you get it evaluated? Does the evaluation help a product in the marketplace? Why or why not?
7. Every country participating in the computer product security evaluation has a list of evaluated products. Find out how to find this list. Does the ISO keep a global list of evaluated products?
8. Why is the product rated as B2/B3/A1 better than that rated C2/B1, or is it?
9. Study the rating divisions of TCSEC and show how product ratings can be interpreted.
10. What does it mean to say that a product is CC or TCSEC compliant?

Advanced Exercises

1. Research and find out if there are any widely used computer product security evaluation criteria.
2. Using the product evaluation list for computer products, determine the ratings for the following products: DOS, Windows NT, 98, XP, Unix, and Linux.
3. Study the history of the development of computer product security evaluation and suggest the reasons that led to the development of ISO-based CC.
4. Study and give the effects of ISO on a criterion. Does ISO affiliation have any impact on the success of a criterion?
5. Does the rapid development of computer technology put any strain on the existing criteria for updates?
6. Study and compare TCSEC, ITSEC, and CC assurance levels.
7. Trace the evolution of the security evaluation criteria.
8. Discuss how standards influence the security evaluation criteria.

References

1. Wikipedia. http://en.wikipedia.org/wiki/Open_standard
2. Bradner S. FRC 2026: the internet standards process—revision 3. Network Working Group. https://tools.ietf.org/html/rfc2026
3. Mercuri R. Standards insecurity. Commun ACM, December 2003, 46(12) 21–25
4. Computer Security Evaluation FAQ, Version 2.1. http://www.faqs.org/faqs/computer-security/evaluations/
5. An Oracle White Paper. Computer security criteria: security evaluations and assessment, July 2001. http://otndnld.oracle.co.jp/deploy/security/pdf/en/seceval_wp.pdf
6. Oracle Technology Network. Security evaluations. http://www.oracle.com/technetwork/topics/security/security-evaluations-087427.html
7. Department of Defense Standards. Trusted computer system evaluation criteria. http://www.iwar.org.uk/comsec/resources/standards/rainbow/5200.28-STD.html