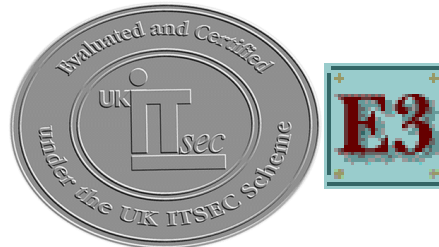


Computer Security Criteria: Security Evaluations and Assessment

An Oracle White Paper
July 2001



This product is rated B1 by NSA in accordance with the Trusted Computer System Evaluation Criteria when installed as prescribed.



This product is rated C2 by NSA in accordance with the Trusted Computer System Evaluation Criteria when installed as prescribed.

This page intentionally left blank

Computer Security Criteria and Security Evaluations

INTRODUCTION

The advent of the Internet is changing the manner in which business is being conducted around the world. This Internet-driven world, as a direct influence on the increasing reliance on information technology (IT), necessitates well-implemented and comprehensive security mechanisms in products and systems alike. Fundamental security issues such as authentication, encryption, protection of data, user privileges, audit and network security still occupy center stage in such a dynamic computing environment, but so do innovations in IT security fraud.

Purchasers need to obtain products and systems that meet their business requirements. Vendors need to design and develop secure products and systems keeping in mind the rapidly changing nature of IT environment and threats.

- But how do buyers shop for products from a security-conscious perspective?
- What are the measures or yardsticks against which a product can be measured in terms of its strengths of its security mechanisms?
- What and where is the proof of claims that a vendor makes about robust security in his products?

This is where security evaluations and security assessment play a critical role in establishing the assurance of a product's security-worthiness. Security evaluations provide a formal yardstick against which a product or system can be certified as having met internationally developed and recognized security standards by independent but authorized and accredited organizations. Security assessment is a less formal security evaluation practice, but equally important in that it provides a mechanism by which vendors independently assess their products' security-worthiness, although not against formal evaluation criteria and/or standards.

Security evaluations provide assurance in the security of Information Technology (IT) products.

SECURITY EVALUATIONS

Security evaluations by independent organizations provide assurance in the security of Information Technology (IT) products and systems to commercial, government, and military institutions. The growth of the Internet and Electronic Commerce, as a direct influence on the increasing reliance on IT, necessitates independent security evaluations to provide an accurate assessment of the strength of security mechanisms in IT products and systems. Such evaluations and the criteria upon which they are based serve to establish an acceptable level of confidence for IT purchasers and vendors alike. Furthermore, security evaluation criteria and ratings can be used as concise expressions of IT security requirements.

Oracle Corporation, as the leading supplier of secure database technology, has successfully completed several formal independent security evaluations of its Oracle7, Trusted Oracle7 and Oracle8 database server products against US, European, International, and Russian evaluation criteria. Oracle is currently involved in security evaluations of its Oracle8 and Oracle8i database server products.

Oracle has made a substantial investment in contracting and supporting security evaluations to ensure that users of Oracle's database server products have the level of assurance they require in the products' secure design, implementation, and functionality. Additionally, systems integrators will be better positioned to incorporate these commercial off-the-shelf products into integrated secure systems which require such levels of assurance.

There are two important components of IT 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.

Security Evaluation Criteria

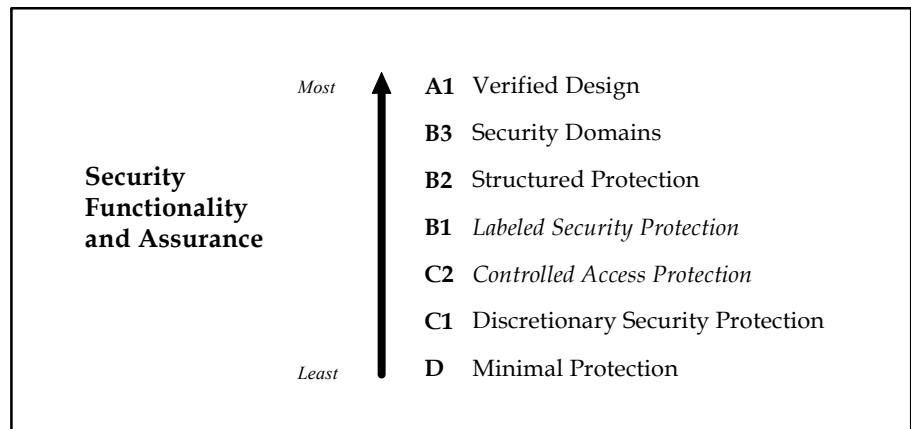
Security evaluations require objective and well-defined evaluation criteria and methods. There are several versions of such criteria and methods recognized internationally. These criteria are described in the following sections in chronologically ascending order - that is, from the oldest criteria to the most recent criteria.

US TCSEC

The US Trusted Computer System Evaluation Criteria (TCSEC or "Orange Book") is used for evaluation of secure operating systems.

First published in 1983, the US *Trusted Computer System Evaluation Criteria* (the TCSEC, also known as the *Orange Book*) was used for the evaluation of operating systems. In April 1991, the US National Computer Security Center (NCSC) published the *Trusted Database Interpretation* (TDI) which set forth an interpretation of these evaluation criteria for database management systems and other layered products.

The TCSEC and the TDI enumerated security evaluation criteria primarily for US government security requirements, concentrating on the need to protect the confidentiality of information. The criteria were helpful for government and commercial organizations that had unclassified but sensitive data.



U.S. ORANGE BOOK CLASSES

Products were evaluated against the TCSEC and the TDI at predefined classes from D (minimal protection) up to A1 (highest protection). These classes represented fixed bundles of functionality (security mechanisms of the product) and assurance (the level of confidence that the security mechanisms functioned correctly and as intended). A product evaluated against the TCSEC or the TDI was given a rating of one of these six Classes. The most relevant Classes for most products were C2 and B1.

C2 -- Controlled Access Protection

A C2 product provides finely-grained discretionary access control (DAC) and makes users individually accountable for their actions through identification procedures, auditing of security-relevant events and resource isolation.

A C2 product provides fine-grained discretionary access control (DAC).

Discretionary access controls restrict access to *objects* (for example, files and tables) based on the identity of the *subject* (for example, a user). Using “need-to-know” policies, an object owner or a security administrator can define which users or groups of users can access specific objects.

In order to achieve a C2 rating, a product must meet these functionality requirements in addition to passing investigations regarding the testing and documentation of the product and its development.

B1 -- Labeled Security Protection

A B1 product provides all the functionality of a C2 product plus mandatory access control (MAC).

A B1 product must contain all the features required of a C2 product and must also be capable of enforcing mandatory access controls (MAC) based on labels. MAC restricts access to data based on the sensitivity (classification) of the data and the formal authorization (clearance) of the user requesting access. If the user is not cleared for the level of classification of the data, access will be denied regardless of any discretionary access rules that may try to grant the user access. Thus, the product must automatically enforce access rules based on sensitivity labels and associate these labels with each user and object within its domain. In a database server this means that objects like tables, individual rows, and each user’s database session are labeled. This type of product security is also called “multilevel security (MLS)” because users and data may be simultaneously present on a shared system at different labels or levels.

In order to achieve a B1 rating, a product must meet these functionality requirements in addition to passing more stringent investigations regarding the testing and documentation of the product and its development. For example, the security policy of the product must be informally or formally modeled.

European ITSEC

The Information Technology Security Evaluation Criteria (ITSEC) was the standard European security evaluation criteria.

The *Information Technology Security Evaluation Criteria* (ITSEC) was the result of the harmonization of the security evaluation criteria of four European nations: France, Germany, the Netherlands, and the United Kingdom. The ITSEC superseded each of their own national criteria and became a de facto European criteria. The ITSEC has been in operational use within European evaluation and certification schemes since July 1991.

Unlike the TCSEC, the ITSEC separated functionality and assurance.

The ITSEC was aimed at evaluations of both products and systems (which may be composed of many secure products and components). Unlike the TCSEC, the ITSEC separated functionality and assurance. A product or system was evaluated against a specific Security Target document which specified the

security functionality of the product or system as well as a claimed evaluation or assurance level.

In contrast to the TCSEC and the TDI, the ITSEC addressed an expanded view of confidentiality, integrity and availability with the aim of more explicitly addressing both military and commercial requirements. The ITSEC defined confidentiality as prevention of unauthorized disclosure of information; integrity as prevention of the unauthorized modification of information; and, availability as prevention of the unauthorized withholding of resources

During the development of the ITSEC, Oracle participated in all the review conferences and responded to all solicitations for comments on draft versions to help ensure the requirements for the evaluation of layered software applications like DBMS servers were addressed by the ITSEC.

Functionality

The Security Target, the guiding technical document of an ITSEC evaluation, defined the security functionality of the product or system by referencing the ITSEC predefined functionality classes, or by specifying individual functionality claims, or both.

Annex A of the ITSEC contains several examples of predefined functionality classes. These include classes which map to the US TCSEC Classes, for example F-C2 and F-B1, which are equivalent to C2 and B1, respectively. There are no predefined functionality classes for some aspects of general purpose relational database servers like data integrity and availability.

Assurance

The ITSEC defined assurance as an important measure of how well the product or system performed in compliance with its claimed security mechanisms. Assurance was measured by correctness of implementation as well as effectiveness of the product or system's security functions and mechanisms.

The ITSEC defined seven such evaluation levels from E0 through E6, representing degrees of confidence in the correctness of the product or system. Level E1 represented an entry point below which no useful confidence could be held, whereas Level E6 represented the highest level of confidence and required very stringent formal development, verification and distribution methods significantly beyond the scope of commercially available products or systems..

Therefore, under the governance of the ITSEC, a product or system was given an evaluation or assurance level (e.g., E3) which represented the level of confidence users could have in the product's or system's provision of the functionality claimed in its Security Target.

Additional North American Criteria

The *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC) was drafted with influences from the TCSEC and the ITSEC. The *US Federal Criteria* was also developed at the same time. This effort was viewed as the first step towards a more unified North American criteria, the elements of which have now been incorporated into the recently-developed and International Standards Organization (ISO)-approved *Common Criteria*.

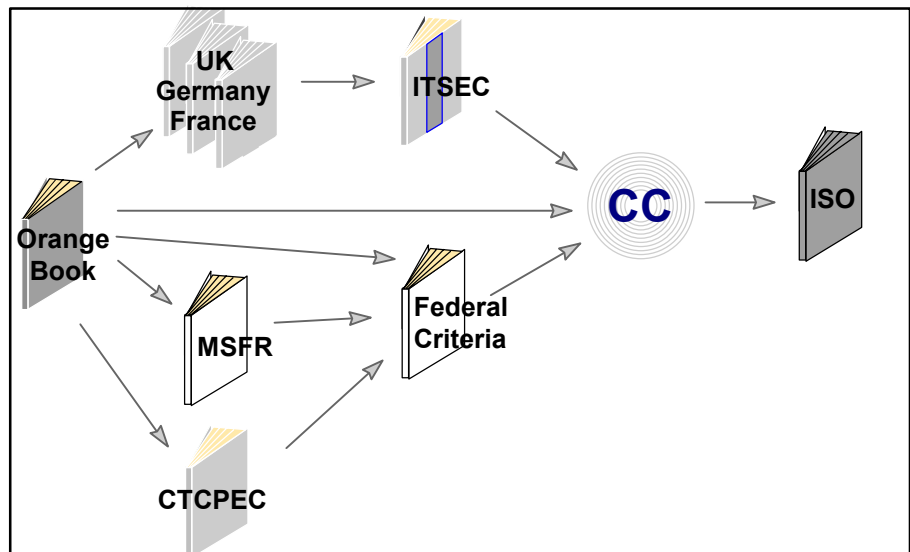
International Common Criteria

The International *Common Criteria for Information Technology Security Evaluation* (referred to as the *Common Criteria*, CC) is a joint effort between North America and the European Union to develop a single set of internationally recognized security criteria. Recently finalized as an ISO standard (number 15408), the CC supersedes the US TCSEC, the European ITSEC, and the Canadian CTCPEC. It is the de facto international security evaluation criteria.

The Common Criteria is a joint effort between North America and several European countries to develop a single set of internationally recognized security evaluation criteria.

Toward International Criteria Harmonization

As security evaluation criteria evolved in the past decade, they moved towards greater flexibility in the specification of the target of evaluation, its relevance in government and commerce, and concentrated on system evaluation issues where a number of different products can be integrated. These were valuable trends which helped ensure the availability of functional and independently-assured products to the largest numbers of users.



EVOLUTION OF SECURITY CRITERIA

While the proliferation of criteria stimulated discussion and progress in important technical and method issues, it placed a burden on international purchasers and vendors. It required security-conscious purchasers to be familiar with a number of security evaluation criteria. It also required security-conscious vendors to be prepared to undertake evaluations of the same products against various criteria and under different evaluation schemes. The CC reduces such onerous requirements and has thus emerged as the worldwide standard with the major objective of mutual recognition of CC evaluation certificates by participating countries.

The CC is the worldwide standard for security evaluation criteria.

To this effect, an *Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security* was formally signed in October 1998. The purpose of this arrangement was to advance that objective by having the nation signatories accept each others' CC certificates without the need for re-evaluation of a product in each country, thereby preventing duplication of evaluation efforts. The arrangement states the grounds for each nation's confidence in the reliability of the judgments on which the original certificate was based by declaring that the Certification (or Validation) Bodies associated with the signatory nations to the arrangement meet high and consistent standards of security evaluations. It specifies the conditions by which each participant accepts results of security evaluations and the associated certifications conducted by other participants, and provides for other related cooperative activities.

As does the ITSEC, the CC addresses an expanded view of confidentiality, integrity and availability with the aim of more explicitly addressing both military and commercial requirements. Information security, once largely the concern of governments and the military, has, with the advent of the Internet, become a great concern to all types of commercial organizations contemplating e-business. Commercial enterprises can also benefit from the same type of assurance that governments demand for formal evaluation of commercial software products and systems.

The CC separates functionality and assurance, as does the ITSEC.

As does the ITSEC, the CC separates functionality and assurance. A product or system is evaluated against either a specific Security Target (ST), the primary technical guiding document of the CC which specifies the security functionality, or a Protection Profile (PP), which is a high-level document targeted at a desired assurance level.

Functionality

The sponsor (or vendor) primarily defines the security functionality of the product in a Security Target or a Protection Profile which is decoupled from the desired assurance level.

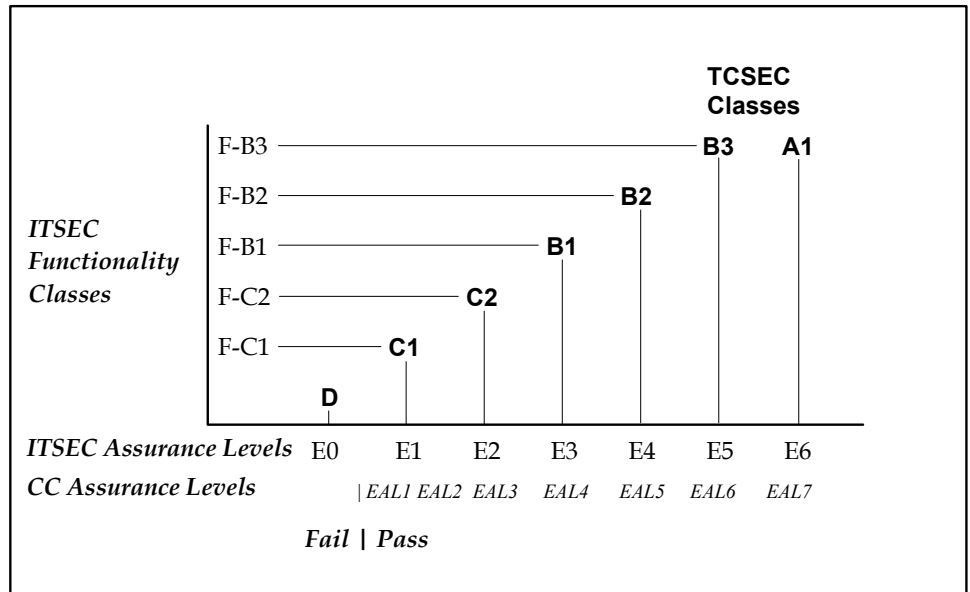
Assurance

The CC also defines assurance as an important measure of how well the product or system performs in compliance with its claimed security. Assurance is measured by correctness of implementation as well as effectiveness of the product or system’s security functions and mechanisms. The CC defines seven such evaluation levels from EAL1 through EAL7 representing degrees of confidence in the correctness of the product or system.

Level EAL1 mandates a minimum of functional testing. Level EAL4 requires the specification of a Security Target, an informal description of detailed design, functional testing, source code analysis, testing of security mechanisms, configuration control systems and approved product distribution procedures. Level EAL7 represents the highest level of confidence and requires very stringent formal development, verification and distribution methods significantly beyond the scope of commercially-available products or systems.

In a manner similar to that of the ITSEC, the effectiveness of a product or system is assessed through a variety of analyses which investigate, for example, the suitability of mechanisms in the product or system for the security objectives of the product or system. Based on an analysis of the strength of all critical security-enforcing mechanisms (like password mechanisms), the product or system is also given a minimum strength of mechanism rating.

Therefore, in CC evaluations, a product or system is given an evaluation or assurance level (e.g., EAL4) which represents the level of confidence users can have in the product’s or system’s provision of the functionality claimed in its Security Target or Protection Profile.



A COMPARISON OF TCSEC, ITSEC & CC ASSURANCE LEVELS

Evaluation Schemes

The process of performing IT security evaluations against evaluation criteria differs according to the relevant sanctioning body. The differences in these processes affect the roles of the evaluators, sponsors, and developers; the cost and duration of the evaluations; and, the resources required to perform and support the evaluations.

US TCSEC Evaluation Scheme

The National Computer Security Center (NCSC) performed security evaluations in the US.

The US National Computer Security Center (NCSC), part of the National Security Agency (NSA), performed security evaluations in the US. Evaluations were performed under the aegis of the Trusted Product Evaluation Program (TPEP) and products successfully completing the program were given a TCSEC Class rating and placed on the US Evaluated Products List (EPL).

The TPEP has now been officially desupported by the NSA and products are not being accepted for any new TCSEC evaluations.

European ITSEC Evaluation Scheme

Commercial Evaluation Facilities (CLEFs) perform evaluations against ITSEC, with the oversight of a government body.

In the UK, Commercial Evaluation Facilities (CLEFs) perform evaluations within the UK IT Security Evaluation and Certification Scheme. Oversight of the scheme is conducted by a government body known as the Certification Body (CB) which is operated by the Communications-Electronics Security Group (CESG).

The ITSEC scheme also clearly defines the process of how to evaluate products, and this is published in the IT Security Evaluation Methodology (ITSEM).

At the successful completion of an evaluation, the Certification Body issues a certification report and certificate.

At the completion of a successful ITSEC evaluation, the CB issues a certification report and a certificate based upon the findings of the CLEF and its own analysis. The product or system receives an evaluation and assurance level rating and is placed in the UKSP06, a listing similar to the US EPL.

The ultimate goal of the ITSEC harmonization effort of great import to vendors and purchasers alike, is to achieve international mutual recognition of these certificates to ensure that an evaluation successfully performed in Germany, for example, will be recognized in the UK. In April 1996, the US National Institute of Standards and Technology (NIST) published a bulletin which allowed US government procurement agencies to purchase ITSEC F-C2/E2 (or better), or CTCPEC C2/T1 evaluated systems in lieu of US-evaluated systems if the required products were not available on the US EPL.

Furthermore, in November 1997, the Senior Officials for Information Security (SOG-IS) of the European Commission approved *the Recognition Agreement of Information Technology Security Evaluation Certificates* based on ITSEC. The Agreement came into effect in March 1998, and now covers France, Finland, Germany, Greece, Italy, the Netherlands, Norway, Spain, Sweden, Switzerland

and the UK. These nations agree to recognize ITSEC certificates from qualifying Certification Bodies, which initially are SCSSI of France, BSI of Germany and CESG of the UK.

International CC Evaluation Scheme

The goal of the CC evaluation scheme is worldwide mutual recognition of certificates.

The CC follows a scheme similar to that of the European ITSEC. It is overseen by the CESG in the UK, by the NSA in the US, and by the respective governing bodies of each of the countries participating in the CC.

Products completing a successful CC evaluation are given an evaluation assurance level rating and placed on a Certified Products List.

One of the initial tenets of the development of the CC was the worldwide recognition of certificates. To this end, the International Standards Organization (ISO) has adopted Version 2.1 of the CC as an ISO standard, number 15408.

Other Evaluation & Certification Schemes

Oracle also participates in other validation and evaluation schemes.

In addition to the evaluations schemes mentioned in the preceding sections, Oracle has also participated in other evaluation criteria and their respective schemes.

US Federal Information Processing Standard

The *Federal Information Processing Standard (FIPS) PUB 140-1, Security Requirements for Cryptographic Modules*, was established by the US National Institute of Standards and Technology (NIST) and the Canadian Government's Communication Security Establishment (CSE). The FIPS 140-1 standard is jointly maintained by both of these organizations.

Encryption products purchased by US and Canadian government agencies may be required to undergo the FIPS 140-1 validation. As such, these products need to be validated against FIPS 140-1 at security levels ranging from level 1 (lowest) to level 4 (highest). Level 2, which requires formal documentation and rigorous testing is the highest security level aimed at by software vendors. Level 4 can be generally only achieved by hardware vendors; for example, hardware encryption devices which need to undergo the even more rigorous documentation, proof and testing required at Level 4.

The testing and validation of products against the FIPS 140-1 criteria is performed by NIST and CSE-approved and accredited certification laboratories.

Russian Federation Certification Criteria and Scheme

The Russian Federation certification criteria and scheme consists of a collection of five guiding documents containing certification rules, levels and standards published and overseen by the government institution, Russian Gostekhkommisssia (Russian State Technical Commission). The security levels of this criteria are IV (lowest), III, II and I (highest).

Oracle has fully embraced the CC as its de facto evaluation criteria and shall thus, not participate in the TCSEC or the ITSEC any more.

Oracle Security Evaluations Status

Oracle has completed multiple security evaluations of Oracle, Trusted Oracle and Oracle Advanced Security on open systems platforms in the US and Europe. Oracle has chosen open systems platforms due to the increasing number of requirements for open secure systems in government, defense, and industry.

Due to the international recognition and acceptance of the CC as an ISO standard, Oracle does not intend to pursue any further TCSEC or ITSEC evaluations. Thus, Oracle has fully embraced the CC as its de facto evaluation criteria and intends to pursue all future evaluations of its database server products against this criteria only.

Oracle was the first database vendor to successfully produce and evaluate a Protection Profile (PP) under the CC. Furthermore, Oracle was also the first vendor of any kind to formally complete a CC EAL4 evaluation of its Oracle7 database server. Since then, Oracle has entered its Oracle8 and Oracle8i database server products into formal evaluation against the CC at EAL4, and has developed and evaluated multiple industry-recognized PPs at high levels of assurance.

Oracle is also the first and only database vendor to successfully complete certification against the Russian Federation security evaluation criteria. However, Oracle will no longer participate in the Russian criteria for evaluation of its database server products.

And, finally, Oracle's cryptographic product, Oracle Advanced Security, successfully completed Oracle's first ever FIPS 140-1 validation at Level 2. Testing of Oracle Advanced Security and its validation against FIPS 140-1 was performed by InfoGard Laboratories, Inc., a NIST- and CSE-approved and accredited certification laboratory in the US.

The table provided in Appendix A summarizes Oracle security evaluation accomplishments and work in progress to date.

System Evaluation and Accreditation Issues

Evaluations of Oracle's server products - Oracle7, Oracle8 and Oracle8i, its MLS server product, Trusted Oracle7, and its cryptographic product, Oracle Advanced Security, provide significant evidence for program certification and accreditation (US), or evaluation and certification (European) of systems incorporating Oracle database servers as important security-enforcing components. For example, in the case of the European evaluations, the Oracle proprietary Evaluation Technical Reports and Certification Reports may be made available to the authorities responsible for evaluating and certifying systems.

The relevance of evidence from previous evaluations depends upon a number of factors, such as the specific assurance requirements of the system, the versions

of the server, the operating system(s), or the hardware configuration being deployed and the server components relied upon to meet the system security policy requirements. These factors may be taken into account in determining whether and how much re-evaluation, re-testing, or additional evaluation work is required to satisfy system assurance requirements, or whether the risk resulting from not performing that additional work can be managed satisfactorily.

For example, since all the security evaluation criteria examine Oracle's IT environment and procedures for the design, development, testing and porting of its products, a reasonable amount of confidence results from the success of these evaluations which can be sufficient in proving that: 1) the same release of an Oracle database server will work securely on different hardware configurations running the same operating system or, 2) a different maintenance release of an Oracle database server will work securely on the same or similar operating system or, 3) that a different maintenance release of an Oracle server will work securely on a similar Unix-based operating system.

Related Capabilities

Oracle has evaluated the standard commercial releases of Oracle7 and Trusted Oracle7 in both the US and the UK. This ensures that commercial off-the-shelf (COTS) software meets stringent security requirements. Additionally, many other standards and functionality criteria are also met. For example, both Oracle7 and Trusted Oracle7 have been certified by the US National Institute for Standards and Technology (NIST) to be 100% compliant with the full ANSI SQL 1989 (ISO 9075:1989) standard, including the integrity enhancement feature.

Oracle's evaluated database servers are Year 2000-compliant.

The evaluated releases of the Oracle8, Oracle7 and Trusted Oracle7 database servers are Year 2000 compliant. Oracle self-certifies these versions as Year 2000-compliant (or "Y2K-complaint") in addition to the Year 2000 security checks which are documented in recent ITSEC certification reports.

Trusted Oracle7 contains all the functionality of Oracle plus multilevel security.

Trusted Oracle7 contains the full functionality of Oracle7. Both products provide exceptional DBMS technology capable of providing transparent data sharing across heterogeneous operating systems, network services, transaction processing systems, and other data sources. For more information on these topics see the references in the last section of this paper entitled "Additional Information."

Benefits of Security Evaluations

Security evaluations provide numerous benefits. Any vendor can claim to have security properly implemented and functioning in his product. Independent verification of such claims and a stamp of approval by certified international organizations only strengthens a vendor's reputation for the quality of products so produced.

Furthermore, security evaluations also help in improving the quality of products. Products submitted for security evaluations are subjected to detailed scrutiny at an architectural and code level. Such scrutiny may result in the discovery of architectural vulnerabilities in a product's security mechanisms. Products are also subjected to independent evaluator testing which serves as an additional quality assurance check for potential vulnerabilities in the implementation of a product's security mechanisms. Products do not pass evaluation unless and until all discovered security vulnerabilities are resolved by the vendor. Thus, the end result is a well-tested, security-proven and well-examined product for government or commercial use.

SECURITY ASSESSMENT

One of the drawbacks of the CC, the ITSEC and the TCSEC including the other criteria described in the previous sections, is the cost of a formal evaluation. Another drawback is the length of time that a particular evaluation may take to complete.

A technical complement to security evaluations for independent verification of a product's security claims is *security assessment*. Security assessments are broadly based on well-established security risk assessment techniques and provide an excellent methodology to extract significant security concerns from product vendors in a relatively short period of time.

Security assessments can be performed by an organisation's own security product team or by established third-parties under contractual agreement. The advantage of using established third-parties is that they provide an unbiased and independent assessment of a product or system.

Oracle recently extended the charter of its security evaluations group to include security assessments. Oracle is performing assessments of these products internally and by utilizing the services of independent third-parties under contractual agreement.

The most common types of assessments performed by Oracle are described below.

Product Security Assessment

Product security assessments are generally performed at a theoretical, document-only level. Assessors typically request the vendor whose product is in assessment to supply all available architecture, design and specification documents on the product. The architecture of the product is analyzed for possible security flaws and recommendations are made in a final report which is produced at the end of the assessment.

This type of methodology is rarely used by itself alone. It is used in conjunction with penetration testing and hacking as described by the more comprehensive security assessment methodologies described below.

Penetration Testing

Penetration testing is primarily targeted at network-based software products and systems (e.g., on-line stores, auctioneers, business-to-business e-commerce, etc.). An attempt is made to penetrate and breach the network infrastructure upon which the products and systems are built. Penetration testing mirrors attacks by an external entity (e.g., a hacker) on a target system. Examples of penetration testing include bypassing firewalls, breaching firewall security and

masquerading using false proxies, to mention a few. Penetration testing also warrants system-level architectural analyses.

Product Attacks

Product attacks further complement penetration testing by focusing on a specific product. This technique assumes that an attacker, an external entity or a system insider, has managed to gain console level access to the target hardware (and software). There are two types of product attacks:

- *Black box testing*. This attack attempts to determine what a knowledgeable attacker may achieve by attempting to break the security of a product. The assessment is performed only on the product under attack by analyzing its documentation and other publicly-available information.
- *White box testing*. This attack extends that offered by black box testing by allowing the assessors access to the product's internal know-how such as architecture, specification and design documents and the product's source code itself.

Performing an Assessment

The process of performing a comprehensive assessment using all of the three methodologies described above is similar to that of a security evaluation, but without the production of necessary formal documentation as required by a security evaluation. The other difference between assessment and evaluation is the amount of information available to the assessor. A security evaluation requires an in-depth analysis of the product or system and thus, demands all available product and/or system documentation. A security assessment is much more informal and as such, does not require the same amount of in-depth document. Since the period of time typically required for a security assessment is much less than that required for a security evaluation, assessors tend to use a more practical (hands-on) approach even during the initial stages of a security assessment. Assessors generally:

- Undergo a process of developing an understanding of the product, for example:
 - the product's security features;
 - the product's operating environment;
 - the product's architecture; and,
 - the product's usage.
- Review available sources for known and/or likely vulnerabilities, for example:

- resources on the Internet;
 - results of earlier studies and analyses;
 - known bugs; and,
 - experience with similar products and architectures.
- Design tests using the information gathered and prioritize them based upon the likelihood of exploitation and amount of potential damage caused by such exploitation.
 - Perform the tests described above, and develop additional tests as and when appropriate.

Issue a final report detailing the nature of tests so performed and the results so obtained.

Benefits of Security Assessment

Even though security assessment is an abridged form of security evaluations, it also offers excellent benefits. Security assessment helps improve product security as does security evaluations. The various techniques used by assessors may lead to the discovery of potential or extant security vulnerabilities during an assessment. Typically, assessments are performed during the development of a product. Thus, vendors get the opportunity to fix product security flaws before the product's market release. Even if the product has already been developed and is in government and commercial use, independent discovery of potential and/or extant vulnerabilities and their resolution by rapid vendor response greatly improves a vendor's and product's security-worthiness alike. The end result is a well-tested, thoroughly-examined and security-proven product. Furthermore, security evaluation criteria focuses primarily on operating systems, traditional networks and database servers, but there is no information on assessing the security-worthiness of Internet-based products and new development paradigms such as web programming. Since security assessments do not follow strict security evaluation style guidelines, it allows assessors to think beyond the realm of traditional security evaluation techniques and apply newer and more radical methods of assessment approaches.

Drawbacks of Security Assessment

Even though security assessment offers significant benefits to improve a product's overall quality, the primary drawback of security assessment is that products assessed in this manner cannot be effectively compared for security-worthiness. For example, if different groups of assessors find disparate security vulnerabilities, it is not possible to compare which group does the better job since security assessment lacks formal standards.

WORLDWIDE COMMITMENT TO SECURITY

Security is not limited to only government and military institutions in the age of the Internet. With the ever-increasing reliance on mass data storage in database servers, secure networking, more powerful operating systems and a host of newer Internet-based products and technologies to support modern business processes, the need for verification of product and system security-worthiness has increased tremendously. No longer can purchasers of IT products and systems solely rely on the word of the vendor. An independent but accredited formal or informal yardstick is needed to assure such purchasers that the products and systems they are utilizing are security-proven. Security evaluations and security assessment are two such critical measures.

Oracle is committed to providing its users with independently-assured secure database server products. To this end, Oracle has worked with the sponsors of various evaluation criteria to ensure that their criteria is appropriate for layered software products like database servers. Oracle has also supported efforts toward harmonization and mutual recognition of evaluation criteria and schemes for the benefit of users and vendors alike. The best evidence of Oracle's commitment to security is its extensive undertaking to evaluate its products at its own expense through security evaluations and security assessment and its success in obtaining more high assurance certificates against worldwide security evaluation criteria than any other database vendor.

By adopting both techniques, Oracle has committed itself to ensure the development of high-quality, security-conscious and security-proven products for government, military and commercial needs.

Oracle Corporation's ongoing commitment to current and evolving international security standards places Oracle at the forefront of open secure database technology.

Additional Oracle Product Security Information

<http://otn.oracle.com/deploy/security>

<http://www.oracle.com/ip/solve/continuity/security/>

The table provided on the following page shows the current status for completed and present security evaluation projects.

Direct all inquiries regarding Oracle security evaluations to
seceval_us@oracle.com

Status of Oracle Security Evaluations



	Product	Release	Level	Criteria	Platform	Status
	Oracle8	8.1.7	EAL4	ISO 15408	Solaris 2.6, NT 4.0	Evaluated
	Oracle8	8.0.5	EAL4	ISO 15408	NT 4.0	Evaluated
Criteria	Oracle7	7.2.2.4.13	EAL4	C.DBMS PP	NT 3.51	Evaluated
Criteria	Oracle7	7.2.2.4.13	Trial EAL3	C.DBMS PP	NT 3.51	Completed
	Oracle7	7.3.4.0.0	E3 / F-C2	E3/F-C2	NT 4.0	Evaluated
	Oracle7	7.2.2.4.13	E3 / F-C2	E3/F-C2	NT 3.51	Evaluated
	Oracle7	7.0.13.6	E3 / F-C2	E3/F-C2	Solaris 2.2	Evaluated
ITSEC	Trusted Oracle7	7.2.3.0.4	E3 / F-B1	E3/F-B1	HP-UX CMW 10.16	Evaluated
	Trusted Oracle7	7.1.5.9.3	E3 / F-B1	E3/F-B1	Trusted Solaris 1.2	Evaluated
	Trusted Oracle7	7.0.13.6	E3 / F-B1	E3/F-B1	Solaris CMW 1.0	Evaluated
	Oracle7	7.0.13.1	C2	C2	HP-UX BLS 8.0.4	Evaluated
TCSEC	Trusted Oracle7	7.0.13.1	B1	B1	HP-UX BLS 8.0.4	Evaluated
	Oracle8	8.0.3	IV	Russian Criteria	HP-UX 10.20	Evaluated
Russian	Oracle7	7.3.4	III	Russian Criteria	NT 4.0	Evaluated
FIPS	Oracle Advanced Security	8.1.6	2	FIPS 140-1	Solaris 2.6 SE	Evaluated

Appendix B

Additional Security Evaluations Information

US NSA Publications

To order NCSC documents within the United States, send a written request on company letterhead with a list of the titles and numbers of documents requested to:

National Computer Security Center
Attention: S93
9800 Savage Road
Fort George G. Meade, MD 20755-6000
USA

Orders originating outside the US should be directed to the usual US Department of Defense (DoD) document ordering channels applicable for that country.

<http://www.radium.ncsc.mil/>

US FIPS Publications

To order documents and publications on FIPS standard and validation process, contact NIST at:

National Institute of Standards and Technology
National Technical Information Service (NTIS)
5285 Port Royal Road
Springfield, VA 22161
USA

NIST Orders +1 (703) 605-6000
NIST Fax +1 (703) 321-8547

European Publications

ITSEC

For a copy of the Information Technology Security Evaluation Criteria, send a request to:

Commission of the European Communities

Directorate XIII/F
SOG-IS Secretariat, TR61 02/28
Rue de la Loi, 200
B-1049 Brussels
Belgium

info@itsec.gov.uk

<http://www.itsec.gov.uk/docs/pdfs/formal/ITSEC.PDF>

UK Scheme

For a copy of the description of the UK ITSEC Scheme, send a request to:

UK ITSEC Scheme

Certification Body
PO Box 152
Cheltenham GL52 5UE
United Kingdom

Phone +44 1242 238739

Fax +44 1242 235233

info@itsec.gov.uk

<http://www.itsec.gov.uk/docs/pdfs/formal/UKSP01.PDF>

UK Certified Product List

For a copy of the Certified Product List (UKSP06), send a request to:

UK ITSEC Scheme

Certification Body
PO Box 152
Cheltenham GL52 5UE
United Kingdom

Phone +44 1242 238739

Fax +44 1242 235233

info@itsec.gov.uk

<http://www.itsec.gov.uk/docs/pdfs/guides/products.pdf>

International Publications

International Common Criteria

Information on the CC can be obtained from:

Communications Security Establishment

Criteria Coordinator
R2B IT Security Standards and Initiatives
PO Box 9703, Terminal
Ottawa, Canada, K1G 3Z4

Phone +1 (613) 991-7409

criteria@cse-cst.gc.ca

<http://www.cse.dnd.ca>

Service Central de la Securite des Systemes d'Information

Bureau Normalisation, Criteres Communs
18 rue du docteur Zamenhof
92131 Issy les Molineux
France

Phone +33 (1) 41 46 37 84

ssi20@calva.net

Bundesamt für Sicherheit in der Informationstechnik

Abteilung V
Postfach 20 03 63
D-53133 Bonn
Germany

Phone +49 228 9582 300

cc@bsi.de

Netherlands National Communications Security Agency

Postbus 20061
NL 2500 EB Den Haag
Netherlands

Phone +31 70 348 5637

criteria@nlncsa.minbuza.nl

Communications-Electronics Security Group

CompuSec Evaluation Methodology
P.O. Box 144
Cheltenham GL52 5UE
United Kingdom

Phone +44 1242 221 491 ext 4134

criteria@cesg.gov.uk

<http://www.cesg.gov.uk/>

National Institute of Standards and Technology

Computer Security Division
NIST North Building, Room 426
Gaithersburg, Maryland 20899
USA

Phone +1 (301) 975-2934

criteria@nist.gov

<http://www.csrc.nist.gov/cc>

National Security Agency

Attn: V2, Common Criteria Technical Advisor
Fort George G. Meade, Maryland 20755
USA

+1 (410) 859-4458

common_criteria@rdium.ncsc.mil

<http://www.radium.ncsc.mil/tpep>

Russian Publications

Information on the Russian evaluation criteria can be obtained by writing to:

State Technical Commission

Military Publishing House

03160, Moscow K-160

Small Enterprise "PRINT"

119633, Moscow, Pirechnaya St. 3

Russian Federation

**Computer Security Criteria: Security Evaluations and Assessment
October 2000**

This document is provided for informational purposes only and the information herein is subject to change without notice. Please report any errors herein to Oracle Corporation. Oracle Corporation does not provide any warranties covering and specifically disclaims any liability in connection with this document.

Oracle and Software Powers the Internet are registered trademarks. Oracle7, Oracle8, Oracle8i, Trusted Oracle and Security Without Compromise are trademarks of Oracle Corporation.

ORACLE

Oracle Corporation
World Headquarters
Attention: Security Product Management
500 Oracle Parkway
Redwood Shores, CA 94065
USA.

Worldwide Enquiries:
Phone +1.650.506.7000
Fax +1.650.633.0489
Web <http://www.oracle.com/>

Copyright © Oracle Corporation 1995, 1996, 1997, 1998, 1999, 2000
All Rights Reserved
Printed in the United States of America