

Common Criteria Certification: Apple's Ongoing Commitment to Security

Introduction

Apple has always been committed to providing the safest, most user-centered computing experience possible. Mac OS X is built on a rock-solid UNIX foundation that contains many security features built into its core architecture. Simple user interfaces and configuration tools allow the system to be easily and securely configured. Additionally, the non-proprietary, open source core facilitates analysis and evaluation of the infrastructure, resulting in a robust, more thoroughly tested security foundation.

Due to the rapid growth of the Internet, protecting your data has become more important than ever. In response, Apple has augmented its commitment to security by completing Common Criteria certification for both Mac OS X 10.3.6 and Mac OS X 10.3.6 Server. Achieving Common Criteria certification, a standard method of evaluating the security capabilities of Information Technology products, demonstrates the security of these two operating systems through independent evaluation.

Overview of the Common Criteria

The Common Criteria, an internationally approved set of security standards, provides a clear and reliable evaluation of the security capabilities of Information Technology products. By providing an independent assessment of a product's ability to meet security standards, the Common Criteria gives customers more confidence in the security of Information Technology products and leads to more informed decisions. Security-conscious customers, such as the U.S. Federal Government, are increasingly requiring Common Criteria certification as a determining factor in purchasing decisions. Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings.

The international scope of the Common Criteria, currently adopted by fourteen nations, allows users from other countries to purchase Information Technology products with the same level of confidence, since certification is recognized across all complying nations.

Evaluating a product with respect to security requires identification of the customer's security needs and an assessment of the capabilities of the product. The Common Criteria aids customers in both of these processes through two key components: protection profiles and evaluation assurance levels.

Protection Profiles

A protection profile defines a standard set of security requirements for a specific type of product (e.g. operating systems, databases, firewalls, etc.). These profiles form the basis for the Common Criteria evaluation. By listing required security features for product families, the Common Criteria allows products to state conformity to a relevant protection profile. During Common Criteria evaluation, the product is tested against a specific protection profile, providing reliable verification of the security capabilities of the product.

Since Information Technology products can be linked to specific protection profiles, customers can compile a list of critical security features by examining the details of a relevant protection profile. In addition, since the Common Criteria certification verifies that a product meets the requirements of a protection profile, customers can rapidly assess the product's ability to meet their security needs, and compare the security capabilities of any validated products.

Evaluation Assurance Levels

In addition to protection profiles, a vendor may choose an Evaluation Assurance Level (EAL1-EAL7), a measure of the depth of engineering review and evaluation of the product lifecycle itself. Unlike protection profiles, the EAL does not indicate the actual security capabilities of the product, but independently stipulates the level of evidence reviewed and functionally tested against the vendor claims.

The Certification Process

The purpose of product certification is to provide customers with a high level of trust, which requires a thorough, reliable, objective, and globally accepted process. To submit a product for certification, the vendor must first specify a Security Target (ST). The ST description includes an overview of the product, potential security threats, detailed information on the implementation of all security features included in the product, and any claims of conformity against a Protection Profile at a specified EAL. The vendor must submit the ST to an accredited testing laboratory for evaluation. The laboratory then tests the product to verify the described security features and evaluate the product against the claimed Protection Profile. The end result of a successful evaluation includes official certification of the product(s) against a specific Protection Profile at a specified Evaluation Assurance Level.

Apple and the Common Criteria

Apple subscribes to the Common Criteria Scheme as an effective way to help Information Technology professionals deploy products they can trust. To demonstrate its commitment, Apple submitted both Mac OS X 10.3.6 and Mac OS X 10.3.6 Server for evaluation against the "Controlled Access Protection Profile" (CAPP), which defines the security requirements for commercial operating systems. The certification provided a reliable, independent verification that both Mac OS X 10.3.6 and Mac OS X 10.3.6 Server conform to the CAPP and therefore meet the Apple claimed Security Target. To best meet the needs of its customers, Apple certified to EAL 3, which provided methodical testing and evaluation of the Operating System.

To achieve certification for Mac OS X 10.3.6 and Mac OS X 10.3.6 Server, Apple worked closely with Science Applications International Corporation (SAIC), an internationally recognized testing laboratory with considerable experience evaluating commercial operating systems and McAfee Research, who was engaged to develop the audit infrastructure that is now a part of the Operating System. SAIC has been accredited by the National Information Assurance Partnership (NIAP) as a member of the Common Criteria Evaluation and Validation Scheme for Information Technology Security.

Conclusion

Apple has always been committed to delivering high levels of security in its products. Now, Apple has extended that commitment to include Common Criteria certification for both Mac OS X 10.3.6 and Mac OS X 10.3.6 Server, providing an independent assessment that is internationally recognized and accepted.

Related Links

For further information, please refer to the following resources:

- Science Applications International Corporation (SAIC) evaluation lab home page:
<http://www.saic.com/securebiz/cctl.html>
- National Information Assurance Partnership (NIAP) home page:
<http://niap.nist.gov>
- NIAP Common Criteria Scheme home page:
<http://niap.nist.gov/cc-scheme/>
- International Common Criteria information portal:
<http://www.commoncriteria.org/>
- Common Criteria Overview:
http://www.commoncriteria.org/introductory_overviews/CCIntroduction.pdf
- Common Criteria Introduction and General Model:
<http://www.commoncriteria.org/docs/pdf/CCPART1V21.PDF>