Teknoloji Ürünlerin Güvenlik Açısından Değerlendirmesi

TCSEC, ITSEC, Common Criteria

Afşin TAŞKIRAN // afsin@taskiran.org

www.enderunix.org/afsin | www.taskiran.org

14 Mayıs 2011

Teknoloji pazarındaki ürünlerin çeşitliliği ve üreticilerin çokluğu nedeniyle ürün seçimi de ister istemez zorlaşmakta. Bir çok üreticinin pazara sunduğu teknolojiler, test alanı sınırlı tüketici firmalar tarafından gereğince değerlendirilmeden satınalması yapılmakta. Ürün seçimindeki bu zorluklar ve seçimin daha somut hale getirilme isteği nedeniyle ürün değerlendirilmesinde de standartlaşmaya gidilmiştir. Bu ürün değerlendirme standartlarından bazıları TCSEC, ITSEC ve Common Criteria'dır. Common Criteria günümüzün en geçerli ve yaygın olarak kullanılan değerlendirme standartlarından biridir.

Ürün değerlendirme çalışmaları ilk olarak ABD'de güvenli sistemleri ve vendor ürünlerini değerlendirmek amacıyla **Orange Book (TCSEC)** ile başlamıştır. Orange Book, National Security Agency (NSA) tarafından geliştirilmiş ve tüm ürünler buna göre değerlendirilmiştir. Orange Book (TCSEC)'de D2 ile A3 arasında güvence seviyeleri vardır. D sınıfı en düşük test seviyesinden A sınıfı en yüksek seviyeli değerlendirme methodlarıdır. Orange Book'da sadece confidentiality adreslenmektedir. TCSEC sonrasında **ITSEC** değerlendirme kriteri oluşturulmuştur. ITSEC ise confidentiality nin yanında integrity i de ele almaktadır.

Common Criteria (CC - Ortak Kriterler), ürünlerin güvenlik güvence seviyelerinin belirlenmesi için tasarlanmıştır. ABD, Kanada, İngiltere, Fransa ve Almanya bu kriterlerin oluşturulmasında rol oynamıştır. Türkiye de Türk Standartları Enstitüsü – TSE ile CC yi kullanmaktadır.

Bu programın amacı, ürünlerin güvenlik fonksiyonlarının sağlıklı bir şekilde işlediğini, verilerin işlenmesi sırasında meydana gelen olası hatalarda hassas bilgilerin açığa çıkmadığını en yüksek seviyede güvenceye almaktır. Bu değerlendirme kriterleri ürün sahipleri açısından aynı zamanda uluslararası satış ve pazarlama ölçütü olarak da kullanılmaktadır.

Common Criteria, International Organization for Standardization (ISO) and the International Electrotechnical Commision (IEC) 15408:2007 ve ISO/IEC 18045:2005 olarak da standartlaşmıştır. Common Criteria'nın ilk major versiyonu 2005 yılında v2.3 olarak duyurulmuştur. CC'nin şu anki versiyonu olan 3.1, 3 ana bölümden oluşmaktadır.

1. **Bölüm: Giriş ve Genel Model:** CC'ye giriştir. Genel konsept tanımları yapılır ve IT güvenlik değerlendirme prensipleri üzerinde durulur.
2. **Bölüm: İşlevsel Güvenlik Bileşenleri:** Fonksiyonel bileşenler üzerinde durulur. Target of Evaluation (TOE) da bu bölümde işlenir.
3. **Bölüm: Güvenlik Güvence Bileşenleri:** TOE için güvence bileşenleri bu bölümde işlenir. Protection Profile (PP) ve Security Target (ST) ele alınır. TOE için bir puanlama yapılır ve Evaluation Assurance Level (EAL) seviyesi belirlenir.

Protection Profile (PP)

Ürünün gerektirdiği güvenlik özellikleridir. Protection Profiller fonksiyonel standartları işaret eder ve alıcıların RFP yazımlarında da yardımcı olur.

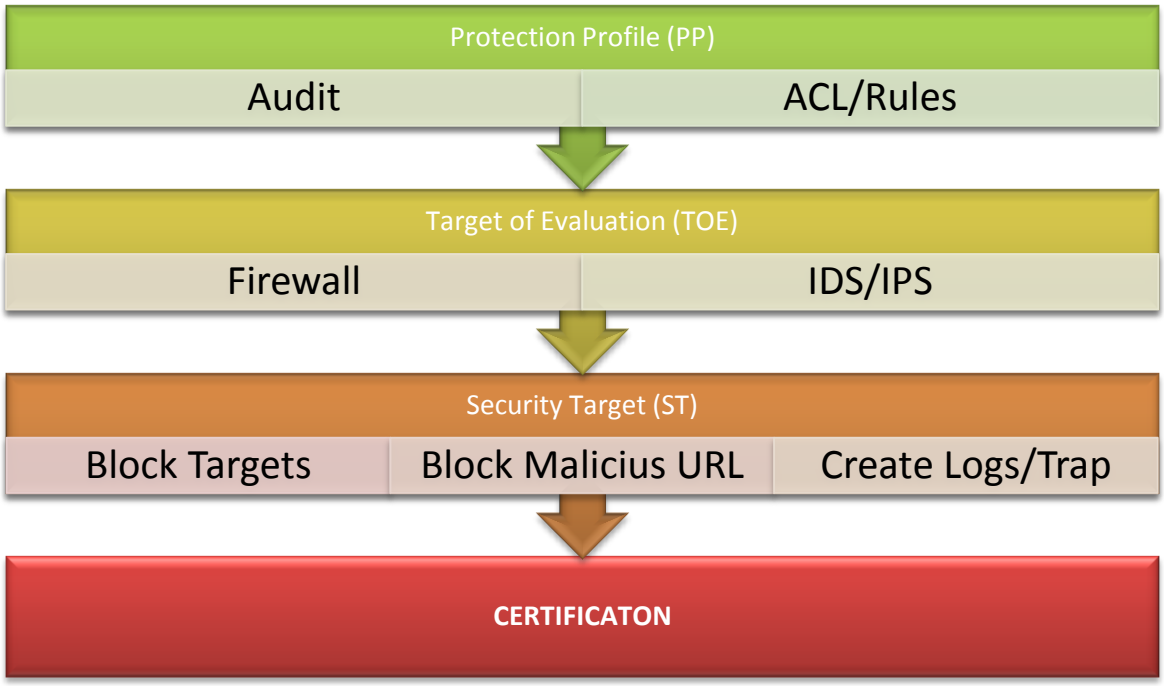
Target of Evaluation (TOE)

Değerlendirilecek olan yazılım, donanım, firmware i adreslemektedir. Bazı TOE örnekleri aşağıdadır.

- Yazılım uygulaması
- İşletim sistemi
- İşletim sistemi ile bütünleşik yazılım
- İşletim sistemi ve iş istasyonu ile bütünleşik yazılım
- Smart karta entegre devre
- Smart karta entegre şifreleme devresi
- Terminalleri, sunucuları, ağ ekipmanlarını ve yazılımları içeren yerel ağ
- Veritabanı uygulaması
- Güvenlik duvarları
- Saldırı tespit ve engelleme sistemleri

Security Target (ST)

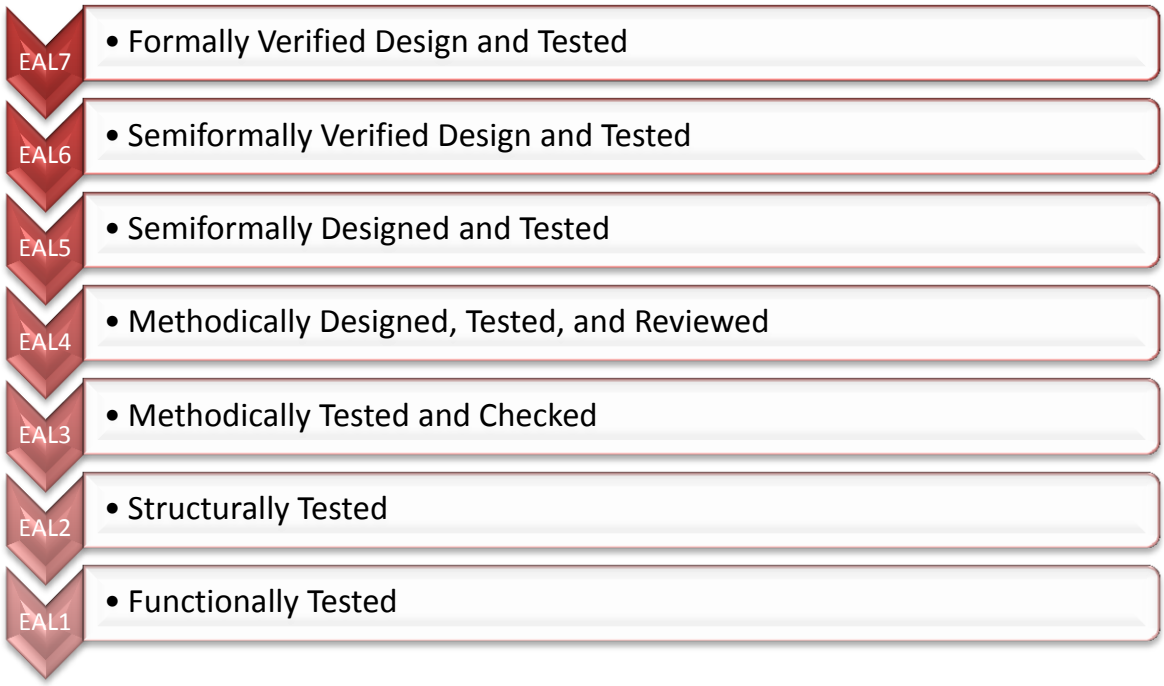
Tanımlanan TOE nin Protection Profile ışığında fonksiyonlarını tanımlar.



Evaluation Assurance Level (EAL 1-7)

EAL; sistemin sağladığı confidentiality, integrity ve availability i ölçmektedir. Implemantasyon sonrası yönetim gibi kriterleri ölçmemektedir. EAL1 en temel, EAL7 ise en kuvvetli seviyedir. Yüksek EAL

seviyesi daha yüksek güvenlik anlamına gelmez, sadece TOE nin kazandığı yüksek güvence seviyesini ifade eder.



Common Criteria sertifikasına sahip ürünlerinin tümünü http://www.commoncriteriaportal.org/products/ adresinden inceleyebilirsiniz.

Kaynaklar:

- Harold F. Tipton, Official (ISC)2® Guide to the ISSAP® CBK, 2011
- Shon Harris, CISSP All-in-One Exam Guide, Fifth Edition, 2010
- Harold F. Tipton, Information Security Management Handbook, Sixth Edition, Volume 3, 2009
- Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2008
- http://www.commoncriteriaportal.org/