

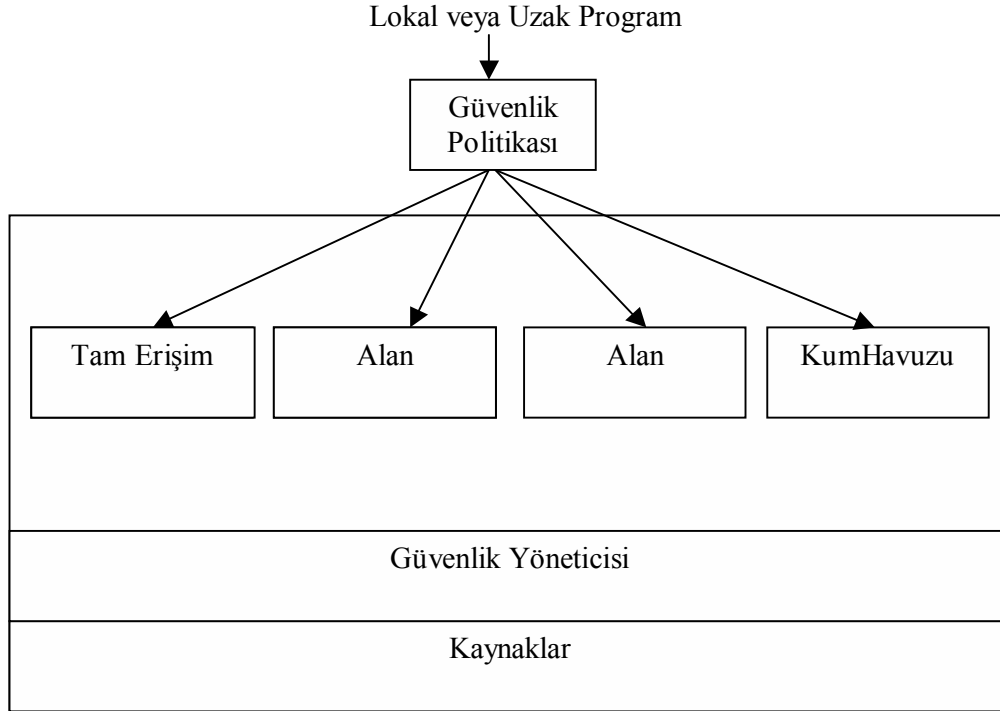
# Java 2 Güvenlik Modeli

Semih Çetinkaya

Uygulama geliştiriciler tarafından kullanılan dillerden biri olan Java ile, mikro ve makro uygulamalar daha kolay, etkin ve güvenli olarak yazılıyor. Bunu sağlayan gelişmiş özelliklerinden biri, güvenlik modelidir.

Java 2 platformu, uygulama geliştiricilerine entegre, esnek ve dağıtık kontrol sağlar. Bu kontrol ile kuruluş, applet, öge, uygulama ve verilerin güvenli olarak oluşturulur.

Java 2 güvenlik modeli, kullanıcılar, gruplar ve uygulama elemanları için politika-bazlı erişim kontrol modelidir. Bu amaçla kullanılabilen üç uygulama aracı vardır: “politika aracı” (policy tool), güvenlik politikalarını tanımlayan politika veritabanlarını oluşturmak ve değiştirmek için kullanılan araçtır; “anahtar aracı” (keytool), genel/özel anahtarları yönetmek ve imzalı dijital sertifikaları göstermek, içeri ve dışarı aktarmak için kullanılır; “jar imzalayıcı” (jarsigner) ise dağıtık yazılım öğelerinin dijital imzalarının doğrulanması için kullanılır.



*Java 2 platform güvenlik modeli*

Java platformunun güvenlik çatısı (java.security.\*) kimlik doğrulamada, X.509 v3 standart sertifikalarını destekler. Ayrıca, Java Kriptolama uzantısı (JCE), Java Güvenli Soket uzantısı (JSSE) ve Java kimlik doğrulama ve izin mekanizması (JAAS) güvenlik özellikleri de Java 2 platformuna entegre edilmiştir.

Java 2 platformu, dağıtık işlemlerde güvenli veri servislerinin oluşturulmasına olanak sağlar; örneğin, dijital sertifikaların değiştirilmesi; SSL üzerinden iş akışlarının

yapılması; programlanabilir genel/özel anahtar oluşturulması, saklanması, ve yeniden erişimi; anahtar değişimi, vb.

Java 2 güvenlik modeli “KumHavuzu” (sandbox) modelini destekler, otomatik olarak kullanıcılar, appletler, uygulamalar, ve kaynaklar güvenilir veya güvenilmez olarak tanımlanır. Ayrıca, Java 2 koruyucu “alan”ların (domain) kabul edilmesi ile tam bir güvenli sistem haline gelmiştir. Karmaşık dağıtık uygulamalarda, alan politikaları belirlenmesi ile geliştiriciler modern güvenlik mekanizmalarını kullanabilirler; örneğin, haklar, şifreleme, dijital imzalar ve sertifikalar gibi.

Java 2'nin dağıtık güvenliği, akıllı-kartlardan, anabilgisayarlara kadar uzanan bir platform gibi davranır. Geliştiriciler, altyapıdaki yazılımı/donanımı bilmeden program geliştirebilirler.

Java programlama dili ile kullanılan yazılımların avantajı, yazılımlar yerel bilgisayar kaynakları ile etkileşebilir: kalıcı veri saklama gibi. Bilgi işlem geliştiricileri, en fazla kullanılan öğeleri yerelde saklayarak uygulamalarının performansını artırabilirler. Bu kalıcı veri saklama sırasında, Java2 güvenlik modeli kullanılır.



*Güvenlik temelleri (tanecikli ve genişleyebilen erişim kontrolü sağlarlar)*

Java 2 platformunun önemli özelliklerinden birisi, tanecikli yapıyı desteklemesidir; Java güvenlik gereksinimlerini uygulamaların en alt düzeyine kadar indirgeme yeteneğini geliştiricilere sunar. Uygulama geliştirici, kullanıcıları, grupları, programı ve işletim servisleri, nesne ve öğeleri içeren politikaları, hakları ve erişim mekanizmalarını kullanabilir.

Uygulama geliştiricileri Java 2 platformu güvenlik özellikleri ile daha kolay ve dağıtık yapıda uygulama geliştirebilirler. Böylece, uygulamaların yazılım süresi kısaltılır ve uygulamalar daha performanslı çalışabilir.