# Özellik bazlı şifreleme

Çetin Kaya Koç

Geçen haftaki yazımızın ana fikri çerçevesinde 'farklı şifreleme modellerine' ihtiyaç duyduğumuzu belirttim. Çok kullanıcılı ve dağınık bir sistemde (örneğin, hasta bilgi ve tanı dokümanlarının tutulduğu ve doktor, hemşire ve diğer hastane görevlilerinin ulaşması ve işlem yapması gereken bir sistemde) bir kullanıcı eğer bazı yetki ve özelliklere sahipse bir veriye ulaşma hakkını elde etmelidir.

Böyle bir yapıyı uygulayıp çalıştırabilmek için güvenilir sunucu (trusted server) kullanabiliriz. Kullanıcıya verdiğimiz erişim yetkisi ile onun veriye ulaşmasını sağlarız. Ancak, bu sunucu güvenirliğini kaybettiğinde, tüm verinin mahremiyeti de kaybolur. Klasik bir şifreleme modeli uyguladığımızda ise, birden fazla kullanıcıya farklı anahtarlar vermek ve bu farklı anahtarlarla aynı verinin birden fazla şifrelenmiş halini tutmamız gerekecek. Dolayısı ile genişleyemeyen (unscalable) bir yapı ile karşı karşıya oluruz.

Amacım, önce problemi açıklamak ve sonra bu problemi çözmek için önerilen bir modelden bahsetmekti; adı ciphertext-policy attribute-based encryption. Buna şimdilik 'şifre kurallı ve özellik bazlı şifreleme' diye tercüme edelim; kısaca özellik bazlı şifreleme de diyebiliriz.

Önerilen sistemde bir kullanıcının gizli anahtarı (private key), kullanıcıya ait özellikleri belirten birden fazla karakter dizisi (strings) ile ilişkilendiriliyor. Kullanıcı bir dokümanı şifrelediğinde, o dokümana erişimi bu özelliklerin belirlediği özel bir yapı ile sağlanabileceğini belirtiyor. Açık dokümana erişmek isteyen başka bir kullanıcının yetki ve özellikleri (credentials and attributes) eğer bu özel yapıyı geçebiliyorsa bu kullanıcı dokümanın şifresini açabilir. Bu özel yapı, prensip olarak bir erişim ağacına benziyor. Ağacın yaprakları özellikleri tutuyor ve düğüm noktaları ise eşik lojik kapılarından ibaret. Bir OR veya AND kapısı böyle eşik kapıları yardımıyla kurulabildiği için, istediğimiz erişim kuralları dizgesini uygulayabiliriz. Özellik bazlı şifreleme metotlarını uygulamak için bize gereken açık anahtarlı sistemler ise bilinear dediğimiz grup ikilileri.

koc@sehir.edu.tr