SET ve SSL Nedir?

SSL (Secure Sockets Layer), ağ üzerindeki web uygulamalarında güvenli bilgi aktarımının temini için (bilginin doğru kişiye güvenli olarak iletimi), "Netscape" firması tarafından geliştirilmiş bir program katmanıdır (program layer).

Burada, bilgi iletiminin güvenliği, uygulama programı (web browser, HTTP) ile TCP/IP katmanları arasındaki bir program katmanında sağlanmaktadır. SSL, web sunucularına (Apache vb), bir modül olarak yüklenir ve böylece web sunucuları güvenli erişime uygun hale gelir. SSL, hem istemci (bilgi alan) hem de sunucu (bilgi gönderen) bilgisayarda bir doğrulama (authentication, iki bilgisayarın karşılıklı olarak birbirini tanıması) mekanizması kullanır. Böylece, bilginin doğru bilgisayardan geldiği ve doğru bilgisayara gittiği teyit edilir.

Bilgisayarların birbirlerini "tanıma" işlemi, açık-kapalı anahtar tekniğine (public-private key encryption) dayanan bir kripto sistemi ile sağlanır. Bu sistemde, iki anahtardan oluşan bir anahtar çifti vardır. Bunlardan açık anahtar (public key) herkes tarafından bilinebilen ve gönderilen mesajı "şifrelemede" kullanılan bir dijital anahtardır. (Burada anahtar'dan kasıt, aslında bir şifreleme -kriptolama- algoritmasıdır. Bu algoritma (yani, anahtar) kullanılarak gönderilecek bilgi şifrelenir). Ancak, açık anahtar ile şifrelenen mesaj sadece bu anahtarın diğer çifti olan "kapalı anahtar" (private key) ile açılabilir (deşifre edilebilir). Kapalı anahtar da, sadece sizin bildiğiniz bir anahtar olduğundan, mesaj güvenliği sağlanmış olur. Örnek olarak, size mesaj göndermek isteyen birine kendi açık anahtarınızı gönderirsiniz. Karşı taraf bu anahtarı kullanarak mesajını şifreler ve size gönderir. ªifrelenen mesajı, sadece sizde olan ikinci bir anahtar (kapalı anahtar, private key) çözebilir ve bu anahtarı sadece siz bilirsiniz.

SSL, web sunucusunu tanımak için, dijital olarak imzalanan sertifikalar kullanır. Sertifika, aslında, o organizasyon hakkında bazı bilgiler içeren bir veri dosyasıdır. Aynı zamanda da, kuruluşun açık-kapalı anahtar çiftinin "açık" anahtarı da sertifika içinde yer alır. Sunucu sertifikası da, o sunucuyu işleten kuruma ait bilgiler içeren bir sertifikadır. Sertifikalar, "güvenilir" sertifika kuruluşları tarafından dağıtılır (VeriSign gibi). İstemci bilgisayar, SSL destekleyen bir sunucuya bağlandığı anda, (bu, https:// ile başlayan URL satırları ile gerçekleşir) doğrulama işlemi başlar.

İstemci, kendi açık anahtarını sunucuya gönderir. Sunucu ise, bu anahtarı kullanarak şifrelediği bir mesajı istemciye geri gönderir. Bir sonraki adımda istemci sadece kendinde olan kapalı (private) anahtarı kullanarak gelen şifreli mesajı çözer ve sunucuya geri gönderir. Mesajı alan sunucu ise, bunu kendisinin gönderdiği orijinal mesaj ile karşılaştırır ve eğer iki mesaj "aynı" ise "doğrulama" işlemi başarıyla tamamlanmıştır ve sunucu bu noktadan itibaren "doğru bilgisayarla/kişiyle" iletişimde olduğunu anlar. Daha sonra sunucu istemciye o an gerçekleşen web oturumunda kullanılacak tüm önemli anahtarları gönderir ve güvenli iletişim başlar. Anahtarlar üretilirken kullanılan bazı popüler algoritmalar olarak, DES (Data Encryption Standard), RSA, IDEA verilebilir.

Bunlardan RSA'nın RC4 algoritması (128 bit şifreleme olarak) Netscape ve Internet Explorer'da da kullanılan bir algoritmadır. SET (Secure Electronic Transaction), elektronik

ticarette, internet üzerinde güvenli bilgi aktarımını sağlamak amacıyla aralarında VISA, MasterCard ve IBM'in de olduğu kuruluşlar tarafından geliştirilen bir protokoldür. SET, özellikle on-Lice (gerçek zamanda) kredi kartı bilgileri iletimi için geliştirilmiş bir standarttır. SET, kredi kartı ile yapılan online ödemelerde, bilgilerin internet üzerinden aktarımında gizlilik ve güvenlik entegrasyonunu sağlar. SET protokolü sadece müşteri (ürün siparişi veren kredi kartı sahibi) ile sanal dükkan (e-dükkan) ve kredi kartı şirketi arasındaki ödeme fazını şifreler.

SET ile, ödeme işlemine taraf olan herkes (müşteri, dükkan sahibi, kredi kartı şirketi), birbirlerini tanırlar (teşhis ederler, authentication) ve bu ispatlanabilir. "Tanıma" işlemi, SSL'dekine benzer bir dijital sertifikasyon sistemi ile yapılır. Yani, ödeme fazına dahil bütün taraflar kendi kimliklerini belirten dijital bir sertifika kullanır.