ONDOKUZ MAYIS ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

**OpenID Connect Tabanlı Tek Oturum Açma (SSO) Sağlayıcısı**

**Yard. Doç. Dr. Recai Oktaş**
**13061066 – Meryem Saka**

**RAPOR 7**

**Bu hafta proje için;**

- ✓ SSL ve TLS protokolleri **konusunda çalışıldı.**

**SSL (Secure Sockets Layer) & TLS (Transition Layer Security) :**

- Türkçeye **Güvenli Soket Kavramı & Taşıma Katmanı Güvenliği** olarak çevrilmişlerdir.
- Netscape tarafından 1994 yılında geliştirilen SSL protokolü üzerinden 1999 yılında TLS protokolü geliştirilmiştir.
- Aslında her ikisi de aynı işlevi yapmaktadır; internet üzerinden sağlanan **"server"** ile **"client"** arasındaki iletişimin güvenli hale getirilmesi için kullanılırlar. Kısaca veri akışının şifrelenmesi işlemini yapan **kriptolama protokolleri**dir.
- SSL ve TLS **OSI Modeli Uygulama Katmanı (**5.katmanında başlar 6.katmanında çalışır**)** nda ağ bağlantıları verisini şifreler.
- Örneğin; e-posta veri gönderme ya da alma trafiğinde, FTP protokolü ile dosya transferinde, alış-veriş sitelerinde, kredi kartları da dahil kişisel bilgilerin bulunduğu her yerde verilerin şifrelenerek taşınmasında vb. yerlerde kullanılır.
- Gönderilen bilgi yalnızca doğru adreste/alıcıda deşifre edilerek görülebilmektedir.
- http sistemine güvenlik katarak, https sistemini ortaya koyan şifreleme protokolleridir.

**SSL ile TLS arasında fark var mı?**

Evet, TLS ufak farklara sahiptir.

- ✓ Eğer istemcinin herhangi bir sertifikası yoksa;
  TLS protokolü **"**Sertifika Yok**"** mesajı geçebilir.
  SSL ise ayrıca bir uyarı mesajı göndermez.
- ✓ TLS HMAC ve PRF standartlarına göre key üretir.
  SSL ise RSA, Diffie-Hellman veya Fortezza/DMS kullanarak key üretir.

bu farklardan birkaçıdır.

! **Not: Server (Sunucu)**; ağ üzerinde bir bilgiyi farklı kullanıcılara, sistemlere dağıtan donanım.

**Client (İstemci)**; bilgiyi karşılayan-alan kullanıcı, alıcı, istemci taraf.

**OSI Modeli nedir?**

OSI başvuru modeli **ISO** tarafından tanımlanmıştır ve ağ uygulamasında kullanılmaktadır. Farklı ağlar üzerindeki bilgisayarların iletişim kurabilmesi, veri akışı sağlayabilmesi için bir referans noktası oluşturmaya yarar. 2 genel katman (uygulama-taşıma) ve 7 farklı iç katmandan oluşan modeldir.

**X.509 Sertifikası nedir?**

X.509 IETF tarafından RFC-2459 olarak yayınlanan globalleştirilmiş bir sertifika standardıdır. Bu sertifikalar gün geçtikçe geliştirilmiş ve V1, V2, V3 olarak 3 yeni sertifika ortaya konulmuştur. V3 türü sertifika en son çıkarılandır ve diğer ikisinin tüm özelliklerini kapsamaktadır.

**Sertifika;** kişinin açık anahtarının yetkili bir sertifika otoritesi tarafından imzalanmış halidir.

**Proje için gelecek haftada;**

**1.** LDAP sunucu şemaları

**hakkında araştırma yapılacaktır.**

Meryem Saka
13061066
25 Kasım 2016