Bil 452 – Veri İletişimi ve Bilgisayar Ağları

3. Proje

Proje Tanımı

Bu proje kapsamında bir sunucu ve istemci arasında, TCP üzerinde çalışan, güvenli bir bağlantı oluşturmanız istenmektedir. Oluşturacağınız bağlantı, güvensiz ve de dinlenebilir bir ağ üzerinden güvenli bir şekilde dosya transferi yapabilmenizi garanti etmelidir.

Bu projeyi yapabilmek için, gönderici ve alıcı olmak üzere, iki düğüm arasında güvenli biçimde dosya transferi yapan bir kod yazmanız beklenmektedir.

Bu proje en fazla 2 kişilik gruplar halinde yapılabilecektir.

Oluşturacağınız Bağlantı ileYapılması Gerekenler

Bağlantı kurulurken kullanıcıların her ikisinin de birer sertifikası olmalı ve kullanıcılar SSL el sıkışması (SSL handshake) yapmalıdır. Eğer SSL el sıkışması sırasında kullanıcılardan birisinin sertifikası yoksa veya hatalıysa, bunu fark eden program istisna (exception) vererek bağlantıyı reddetmelidir. Bağlantı başarılı biçimde kurulduysa, gönderici tarafında argüman olarak verilmiş olan dosya, alıcıya güvenli ve de hatasız bir biçimde iletilmelidir. Dosya transferi tamamlandığında her iki program da bağlantıyı uygun biçimde sonlandırmalıdır.

Program

Bu projeyi yapabilmek için iki adet programa ihtiyacınız vardır: bir portu sürekli dinleyerek bir istek gelmesini bekleyen ve istek geldiğinde SSL el sıkışması başarılıysa önceden belirlenmiş bir dosyayı ağ üzerinde gönderen bir *gönderici program* ve de istek gönderdikten sonra yapılan SSL el sıkışması başarılıysa kendisine gönderilen veriyi okuyup birleştirerek dosyayı oluşturan bir *alıcı program*. Bu programları istediğiniz dili kullanarak gerçekleştirebilirsiniz.

i) Gönderici Program

Gönderici programınız komut satırından çalıştırılabilir olmalı ve sizin program içerisinde belirlemiş olduğunuz bir portu (örn: 1905) dinlemeye başlamalıdır. Bu porttan kendisine istek geldiğinde, istemci ile SSL el sıkışması yapmalıdır. Eğer SSL el sıkışması başarısız olursa ekrana hata mesajı yazdırıp o istemci ile olan bağlantısını sonlandırmalıdır. SSL el sıkışması başarılıysa önceden belirlenmiş olan dosyanın adını ve kendisini istemciye yollamalıdır. Her iki durumda da gönderici program gelebilecek yeni isteklere karşı portu dinlemeye devam etmelidir.

Gönderici program, SSL el sıkışmasından sonra alıcının açık anahtarını (public key) ve sertifika tipini ekrana yazdırmalıdır.

Örnek:

```
-Public Key-
Sun RSA public key, 1024 bits
  modulus:
157970432016068838035652269532125618235745265894445424675194269454115549358253965259105461775503616008346394713985184775421775122360876901515648087577222749003209245621456971220915485313614762697976445525574948396103538720875283987342646171425583799383586661156078212601480243272408887223128621241158480547931
  public exponent: 65537
-Certificate Type-
 X.509
```

ii) Alıcı Program

Alıcı programınız da benzer biçimde komut satırından çalıştırılabilir olmalıdır.Alıcı program çalışmaya başladıktan sonra ilk olarak gönderici durumundaki sunucunun IP bilgisini kullanıcıya sormalı ve kullanıcının klavye ile girdiği sunucu IP adresini kullanmalıdır.

Alıcı program, gönderici programda olduğu gibi, SSL el sıkışmasından sonra göndericinin açık anahtarını (public key) ve sertifika tipini ekrana yazdırmalıdır.

Dosya transferi sonucunda alınan dosyanın adı, gönderilen dosyanın adına "_alindi" ifadesinin eklenmiş halidir. örn: Gönderilen dosya adı "Gizli_Veriler.txt" ise alınıp oluşturulan dosyanın adı "Gizli_Veriler_alindi.txt" olacaktır.

Dosya transferi sonlandıktan sonra hem gönderici hem de alıcı program ekrana

***** DOSYA TRANSFERI BASARILI BICIMDE TAMAMLANDI *****

yazdırmalı ve güvenli bağlantıyı sonlandırmalıdır.

Rapor

Raporunuzda kullandığınız yöntemlerden, kodunuzun güzel olduğunu düşündüğünüz kısımlarından/özelliklerinden, kodunuzun nasıl çalıştırılması gerektiğinden **detaylı biçimde** bahsediniz.

Bunların yanı sıra, hazırlamış olduğunuz güvenli ortamı kullanarak başarılı bir dosya transferinin nasıl olduğunu ekran görüntüleri ile gösteriniz.

Benzer şekilde, oluşabilecek olan istisnaları ve de bu istisnaların oluşma sebeplerini (ekran görüntüleriyle de destekleyerek) detaylı biçimde anlatınız.

Proje Gönderimi

Projenizi **2 Nisan 2015 Perşembe saat 23:59'a** kadar **bil452proje@gmail.com** adresine mail atmanız gerekmektedir. Hazırlamış olduğunuz kodları, .rar veya .zip uzantılı olarak mailinize eklemeli ve mailinizi bu şekilde göndermelisiniz. Maili yollarken konunuzun "[BİL452] Proje 3 Gönderimi - <*öğrenci_numarası*>" olmasına özen gösteriniz.

örn: [BİL452] Proje 3 Gönderimi - 101111041

Yollamanız gereken dosyanın formatı şu şekilde olmalıdır:

Proje3_<*öğrenci_numarası*>/

Rapor.pdf

gonderici.{c, java, pl, ...}

alici.{c, java, pl, ...}

(varsa gerekli ek dosyalar)