BİL 103 – Bilgisayar Bilimlerine Giriş

2. Ödev

Bil 103 dersinin birleştirilmiş 2. ve 3. ödevinde hem soket programlama ile ilgili tecrübe kazanma, hem de güvenli kriptolu haberleşme ve yapılabilecek saldırılar konusunda bilgi sahibi olma ve uygulama yapma imkanınız olacaktır. Birleştirilmiş ödev, toplam 20 puan üzerinden değerlendirilecektir.

1. Kısım (5 puan):

Bir istemci-sunucu mimarisi üzerinden TCP veya UDP (ikisinden birini tercih edebilirsiniz) kullanarak kredi kartı bilgilerinin gönderildiği basit bir ağ uygulaması yazmanız istenmektedir. (Uygulamalarınız tüm programları aynı makinede çalıştırarak test edilecektir). İstemci programı çalıştığında program kullanıcıdan sırasıyla isim-soyisim, kredi kartı numarası, geçerlilik süresi ve güvenlik kodu bilgilerini isteyecek; bu bilgilerin sırasıyla girilmesinin hemen ardından sunucuya gönderecektir. Sunucuda bu bilgileri alacak, girilen isim-soyisim adı ile bir dosya oluşturarak, kalan diğer üç bilgiyi bu dosya içerisinde kaydedecektir. Örnek bir akış şu şekildedir:

> İsim ve soyisminiz:
Ahmet Bulut
> Kredi kartı numaranız:
1234-5678-9012-3456
> Geçerlilik süresi:
05/23
> Güvenlik kodu:
911

Sunucuda "Ahmet Bulut" isimli dosya içeriği şunlar olacaktır:

1234-5678-9012-3456
05/23
911

2. Kısım (5 puan):

Teknik veya teknik olmayan gerekçelerle yukarıdaki uygulamanın doğrudan istemci-sunucu arasında değil de aradaki bir vekil (proxy) sunucu üzerinden gerçekleştirilmesi gerekebilir. Bu durumda işlev aynı kalmak kaydıyla istemci ve sunucu üçüncü bir vekil sunucu üzerinden haberleşeceklerdir (istemci verisini vekil sunucuya gönderecek, vekil sunucu da sunucuya iletecektir). Vekil sunucu üzerinden haberleştiklerini göstermek amacıyla vekil sunucunun aradaki iletişimi anlık olarak (gerçek zamanlı) ekrana basması istenmektedir.

3. Kısım (5 puan)

2. Kısımdaki akıştan da anlaşılacağı üzere eğer ilave bir önlem alınmazsa üçüncü bir taraf (örnek: vekil sunucu) tüm iletişimi dinleyebilir. Ödevinizin bu kısmında Diffie-Hellman anahtar paylaşımı yöntemi ile istemci ve sunucu bir anahtar üzerinde anlaşacaklar ve bu anlaşma ile sağlanan anahtar ile transfer edilen tüm verilerin şifrelenmesi sağlanacaktır. Basit olması açısından Diffie-Hellman anahtar değişimi yöntemi açık parametreleri olarak ondalık düzende (en az) 4 haneli bir p belirlemeniz yeterli olacaktır. Daha sonra uygun bir g değeri de belirleyiniz. Bu değerleri kullanarak daha önce yazmış olduğunuz program üzerinden diğer verileri taşımadan önce Diffie-Hellman anahtar paylaşımı protokolünü işletiniz. Karşılıklı anahtar değişimi sonrası sunucu tarafta elde edilen verileri önce "Ahmet Bulut - şifreli" isimli bir dosyaya yazınız, sonra bu dosyanın şifresini çözerek "Ahmet Bulut" dosyasını oluşturunuz. (Ayrıca sunucu ve istemci tarafta oluşturulan anahtarı oluşturulduktan sonra ekrana basınız.) Şifreleme algoritması olarak istediğiniz bir standart simetrik şifreleme algoritması (AES, DES, vb.) kullanabilirsiniz, fakat kendi algoritmanızı kendiniz tasarlamayınız. Not: Anlaşmış olduğunuz anahtar küçük bir değere sahip olduğu için bu anahtarı bu tür algoritmalarda doğrudan kullanamazsınız. Anahtar uzunluğunu artırmak için bir yöntem geliştiriniz ve bu yönteminizi kodunuzun içerisinde "Python Comment" olarak paylaşınız.

4. Kısım (5 puan)

3. Kısımdaki anahtar değişimi vekil sunucunun yapacağı bir ortadaki adam saldırısına açıktır. Bu saldırıyı gerçekleştiriniz. Bu saldırının yapılmış olduğunu vekil sunucuda yazan programın ekrana basacağı değerler yardımı ile ispat ediniz.

Önemli Not: Arkadaşlar, ödevde pek çok ayrıntının olduğu doğrudur. Fakat belirtmeyi unuttuğumuz önemli hususlar da elbette olabilir. Piazza'da elbette bu hususlar dahil her türlü konuda soru sorabilirsiniz. Ama sorunuzu sormadan önce burada o konuda yeterli bir açıklama olmadığından lütfen emin olunuz. Burada açıklanan hususlar ile ilgili tekrar soru sormanız piazza'daki soru sayısını artırmakta ve sizlerin (ve de bizlerin) soruları ve cevaplarını takip etmesini zorlaştırmaktadır.

Teslim edilecekler:

1. Kısım için: istemci ve sunucu programları: client_1_ ogrencino.py ve server_1_ogrencino.py

2. Kısım için: istemci, sunucu ve vekil sunucu programları: client_2_ ogrencino.py, server_2_ogrencino.py, ve proxy_2_ogrencino.py

3. Kısım için: istemci, sunucu ve vekil sunucu programları: client_3_ ogrencino.py, server_3_ogrencino.py, ve proxy_3_ogrencino.py

4. Kısım için: vekil sunucu programı: proxy_4_ogrencino.py

Ödevinizi tek kişi olarak hazırlayıp 23 Kasım 2020 Pazartesi saat 23:59'a kadar bil103guz2020@gmail.com adresine gönderiniz.