Güvenli Sohbet Uygulaması

Project Proposal Report

BIL548

Giriş

Bu öneri raporu, güvenli bir sohbet uygulaması geliştirmeyi amaçlamaktadır. Proje, bağlantı protokolü, güvenli giriş protokolü, ve güvenli sohbetin implementasyonunu içermektedir. Uygulama implementasyonunda Java 17 ve Maven kullanılacaktır. Aşağıda her bir bölüm detaylı bir şekilde açıklanmıştır.

Nasıl Çalışır?

Server ve Client olmak üzere projenin iki modülü bulunmaktadır.

Sunucu/Server, belirtilen port üzerinde (12345 gibi) çalıştıktan sonra istekleri beklemektedir. Client tarafından gelen isteklere göre cevap dönmektedir. Birden fazla client aynı anda bağlanabilecek şekilde tasarlanmıştır. Her client ayrı thread üzerinde çalışmaktadır ve bağlantılar açık kalmaktadır. Yani her istekte bağlantı açılıp kapatılmaz.

Client, ise sunucunun dinlediği socket üzerinden (12345 gibi) bağlanabilir. Client tarafı kullanıcı gibi çalışmaktadır.

Kullanılacak şifreleme algoritmaları hazır kütüphaneler üzerinden olmaktadır. ECDH için kullanılan kütüphane ekteki gibidir.

```
<dependencies>
    <dependency>
        <groupId>org.bouncycastle</groupId>
        <artifactId>bcprov-jdk15on</artifactId>
        <version>1.68</version>
    </dependency>
 </dependencies>
```

Güvenli Giriş Protokolü

Kullanıcıların uygulamaya girişi kimlik doğrulama protokollerinden (Authentication Protocols) kriptografik yöntemlerle olacaktır. Sunucuların, Client Public Key'ine sahip olduğu varsayılmaktadır.

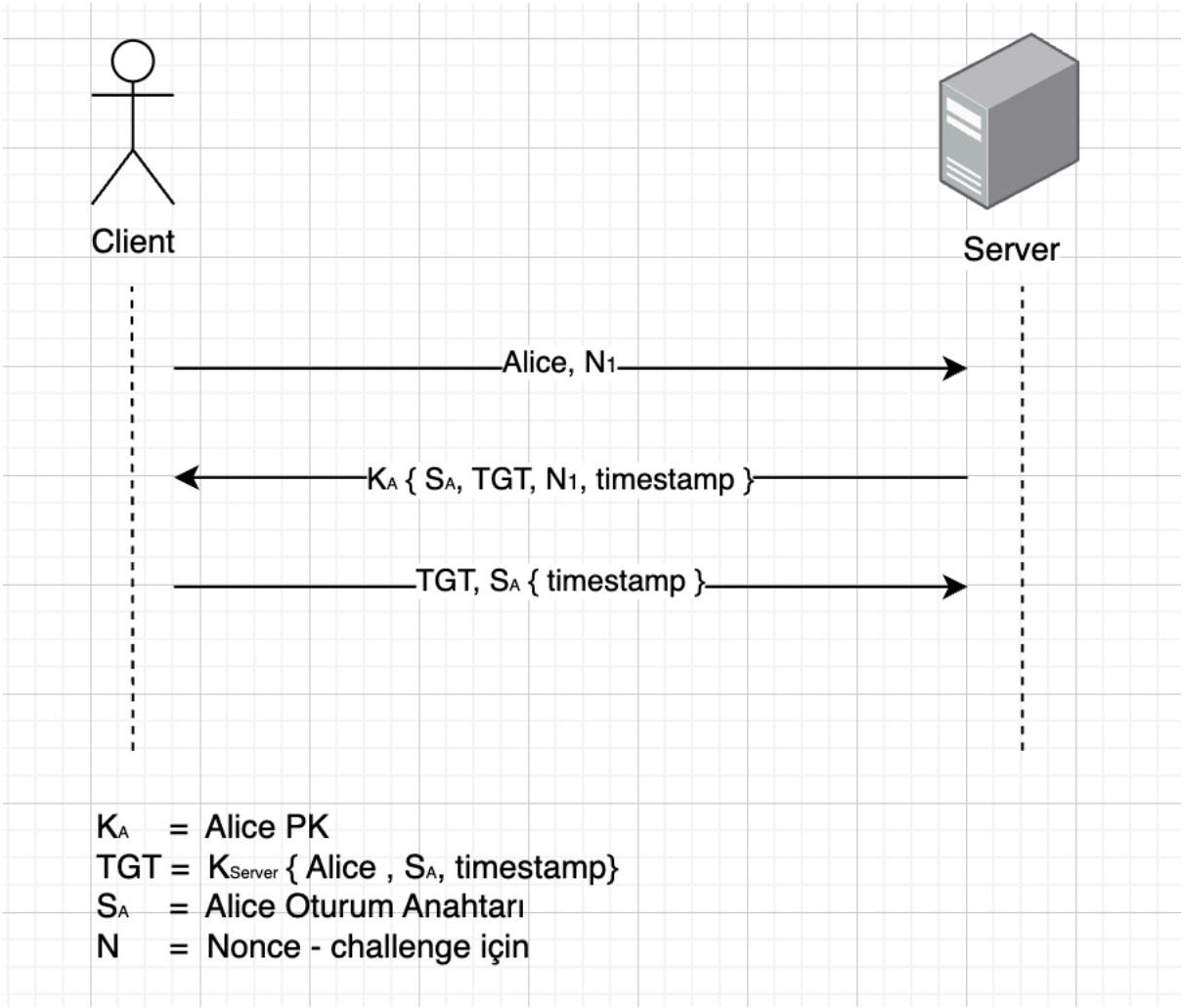

Figure 1 - Güvenli Giriş Protokolü Diagram

Protokol sonunda Client ile Server arasında SA oturum anahtarı oluşur.

1. Client, sunucuya giriş yapmak için ismini ve Nonce değeri yollar
2. Sunucu, kendisinde bulunan client public key ile oturum anahtarını, TGT, N1 ve timestamp şifreleyerek gönderir
    a. Timestamp oturum süreci için eklenmiştir. Belirli aralığı geçmesi durumunda SA'nın yenilenmesi gerekecektir
3. Client kendisinde bulunan private key ile {SA, TGT, N1 ve timestamp} 'yi deşifre eder
4. Sunucuya oturum anahtarı ile timestamp'i şifreleyerek gönderir
5. Sunucu gelen TGT ve şifreli timestamp değerini sunucunun private anahtarı ile açar
6. TGT içindeki SA ile timestamp değerini gelen SA{timestamp} ile karşılaştırır

Bağlantı Protokolü

Alice ile Bob güvenli sohbete başlamadan önce sunucu tarafından sohbet anahtarının belirlendiği protokoldür.

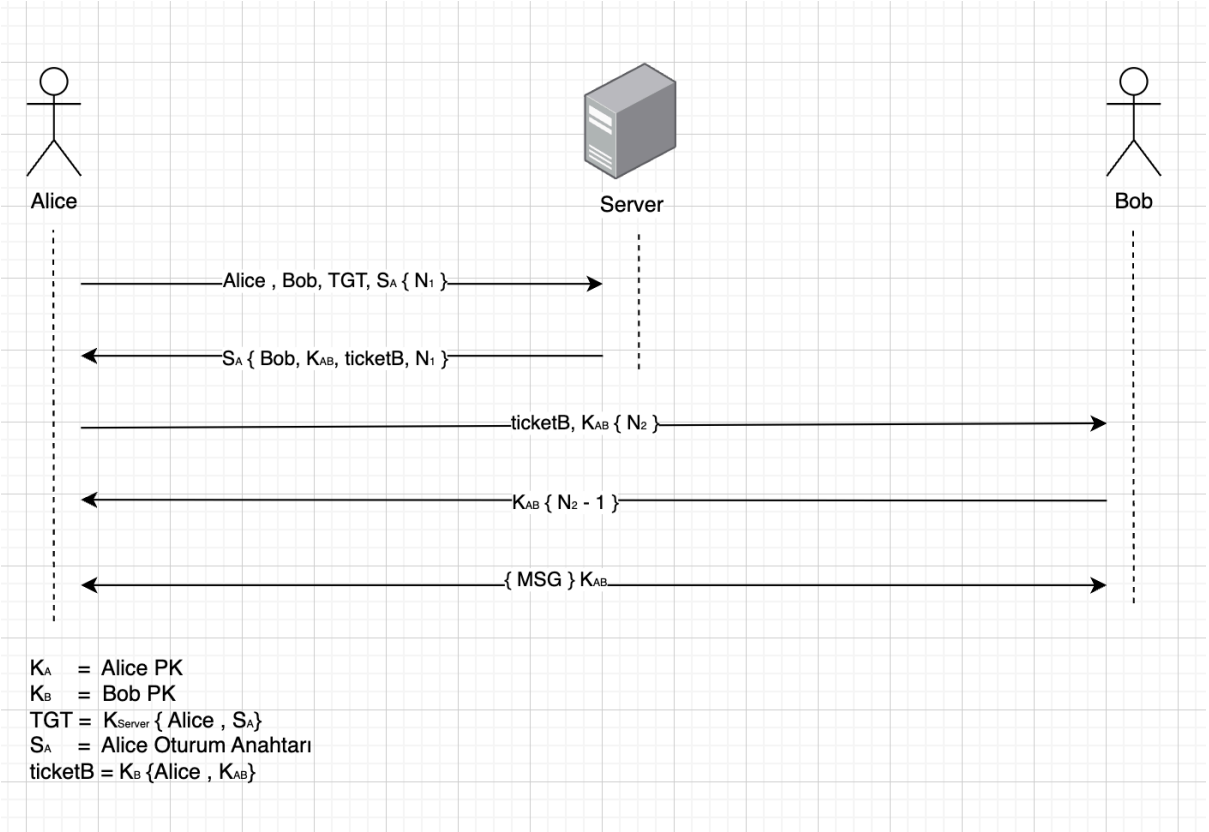

Figure 2 - Bağlantı Protokolü Diagram

Güvenli Sohbet

Güvenli giriş protokolü ve bağlantı protokolü işlemlerinden sonra tüm iletişim bu güvenli hat ve güvenli oturumla bağlanma üzerinden gerçekleşecektir.

Sohbetin güvenliğini teyit için ayrıca MAC ile imzalanacaktır. Böylelikle mesajda herhangi bir değişiklik olmadığı garanti edilecektir.

Güvenli sohbette kullanıcılar, özel sohbetler başlatmak için diğer kullanıcıları davet edebilirler. Bu, kullanıcıların birbirleriyle özel ve güvenli bir şekilde iletişim kurmasını sağlar.

Kaynaklar

- https://github.com/TOBB-University-Master/BIL548 (Source Code)

Güncellemeler

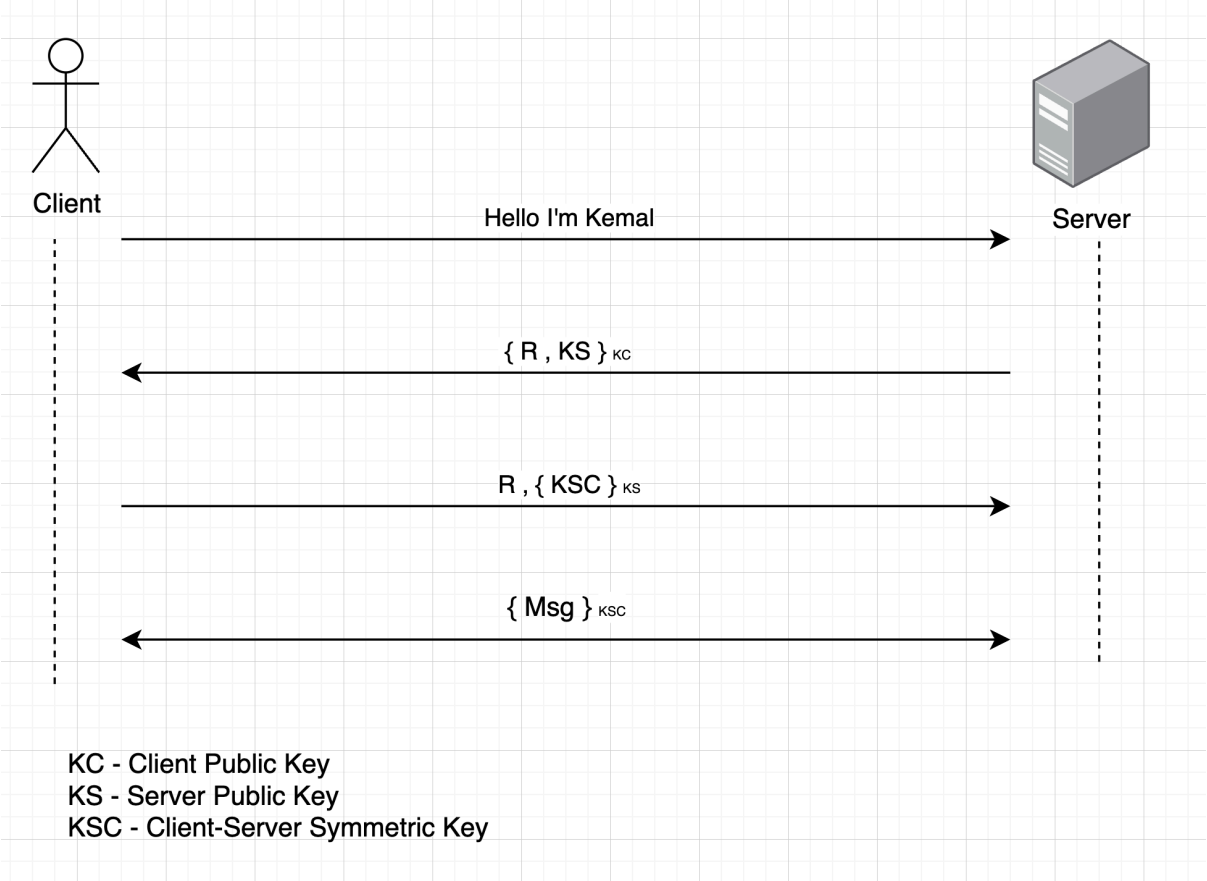

Figure 1 - Güvenli Giriş Protokolü Diagram (Eski)

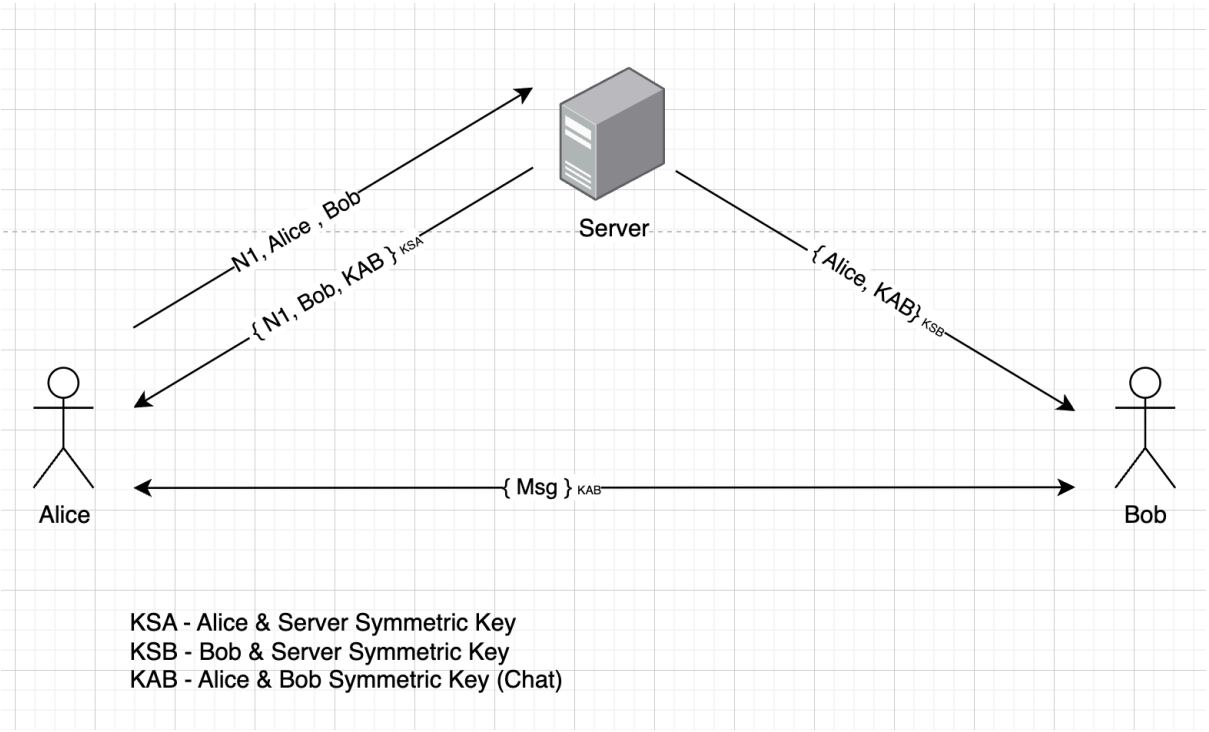

Figure 2 - Bağlantı Protokolü Diagram