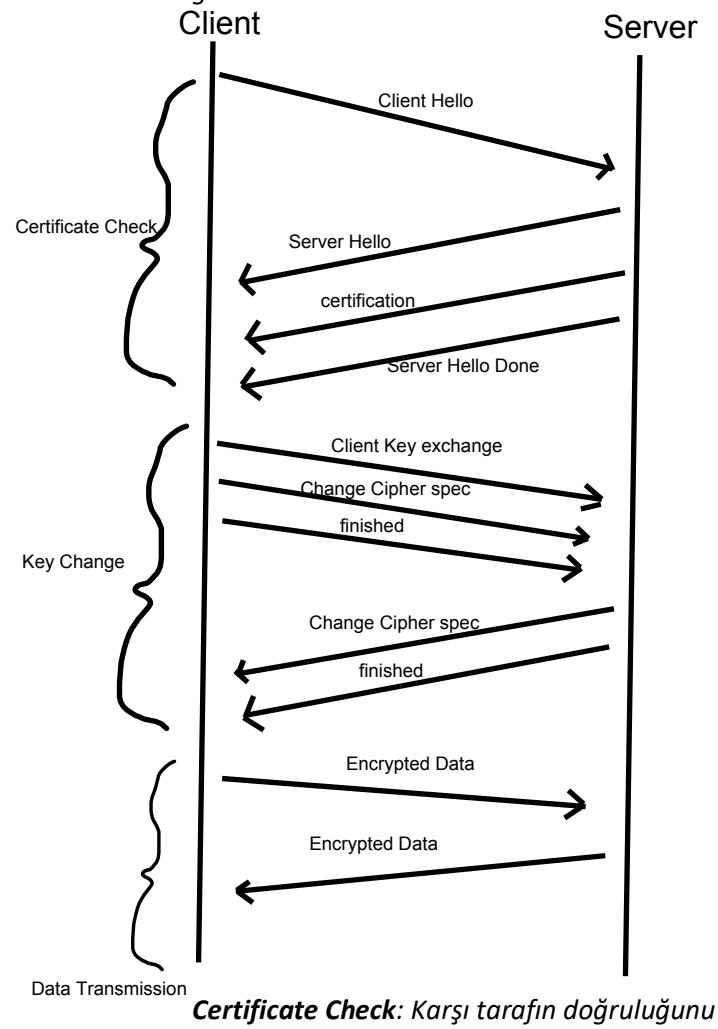
HTTPS HANDSHAKE

Herkese Merhaba, bu yazımda sizlere mülakatlarda sorulabilecek sorulardan birisi olan HTTPS handshake veya diğer adıyla SSL/TLS handshake durumunu lanse etmeye çalışacağım. mülakat sorusu olmasa bile, Siber güvenlik alanında çalışıyorsanız veya ilgileniyorsanız, bilinmesi gereken konulardan birisi diyebilirim. Şunu hatırlatmayalım ki bu anlattığım handshake durumu SSL/TLS 1.2 sürümüne kadar olan handshake durumu, SSL/TLS en son versiyonu olan 1.3 versiyonunda handshake yapısı ve kullanılan asimetrik şifreleme farklı, onu başka bir yazıda ele alacağım. ayrıca SSL/TLS handshake yapısını daha vakıf olabilmek açısınıdan asimetrik ve simetrik şifreleme çalışma prensibini bilmek gerekiyor. buna web sitemden ulaşabilirsiniz.

Aşağıdaki handshake yapısına bakacak olursak, bu handshake yapısını maddeler halinde özetlemek gerekirse.



***Certificate Check**: Karşı tarafın doğruluğunu beyan ettiğimiz ve karşılıklı olarak anlaştığımız adım.*

***Client Hello:** Client, Server'a destekleyebileceği SSL/TLS sürümlerini ve şifreleme listesini karşı tarafa yollar.*

***Server Hello:** Server, Client'a destekleyebileceği SSL/TLS sürümlerini ve şifreleme listesini karşı tarafa yollar.*

***Certification**: Server, Client'a kendisinin sertifaka bilgilerini verir, verilen sertifakada en önemli bilgilerden birisi, Sunucusunu Public Key anahtarıdır*

***Server Hello Done:** Server karşı tarafa iletmiş olduğu Hello done mesajı ile İletişimin ilk adımı tamamlanır.*

Burada certifiaction ile ilgili olan handshake durumunuda bir kaç bilgi vermek istiyorum. server tarafında bize verilen sertifakayı, Sertifaka otoriteleri dediğimiz bir topluluğa soruyoruz, bunun nedeni ise karşı tarafın doğruluğunu teyit etmek. bunu daha da vakıf olabilmek açısından Sertifaka otoriteleri veya Modern Web konusunu bilmek gerekiyor. ama şimdilik bu kısa bilgi ile kalmanız sizin için kafidir.

***Key Change:** Client tarafından oluşturulan secret key karşı tarafa ulaşımı ve anahtar değişiminin gerçekleştiği adım.*

***Client Key Exchange:** Server tarafından verilen simetrik şifreleme listesi üzerinden bir simetrik şifrelem algoritması belirlenir ve bu algoritmaı kullanarak bir secret key oluşturulur, oluşturulan bu secret key, sunucunu bize vermiş olduğu Public Key anahtarı ile şifrelenip,Sunucuya yollanır.*

***Change Cipher Spec(Client):** Client, Server'a belirlemiş olduğumuz simetrik şifreleme algoritması üzerinden data paylaşımına hazır olduğunu beyan eder.*

***Change Cipher Spec(Server):** Server, Client'a belirlemiş olduğumuz simetrik şifrelem algoritması üzerinden data paylaşımına hazır olduğunu beyan eder.*

***Data Transmission:** anlaşmış oldukları simetrik şifreleme üzerinden data transferi gerçekleşir.*

Tabi ki de arka tarafta Client Hello bayrağından önce, TCP üçlü el sıkışması olduğunu gözden kaçırmayalım. Onu başka bir yazımda bahsettim. En sade anlatım biçimiyle SSL/TLS handshake yapısının sizlere lanse etmeye çalıştım.

e-mail

berathanakcakaya@gmail.com

linkedin

https://www.linkedin.com/in/berathan-akcakaya/