GAZİ ÜNİVERSİTESİ

MÜHENDİSLİK FAKÜLTESİ - BİLGİSAYAR MÜHENDİSLİĞİ

171180010 – Cansu AYTEN

BM402 BİLGİSAYAR AĞLARI

ÖDEV 4: Secure Sockets Layer (SSL) ve Transport Layer Security (TLS)

Nisan 2022

İÇİNDEKİLER

Sayfa

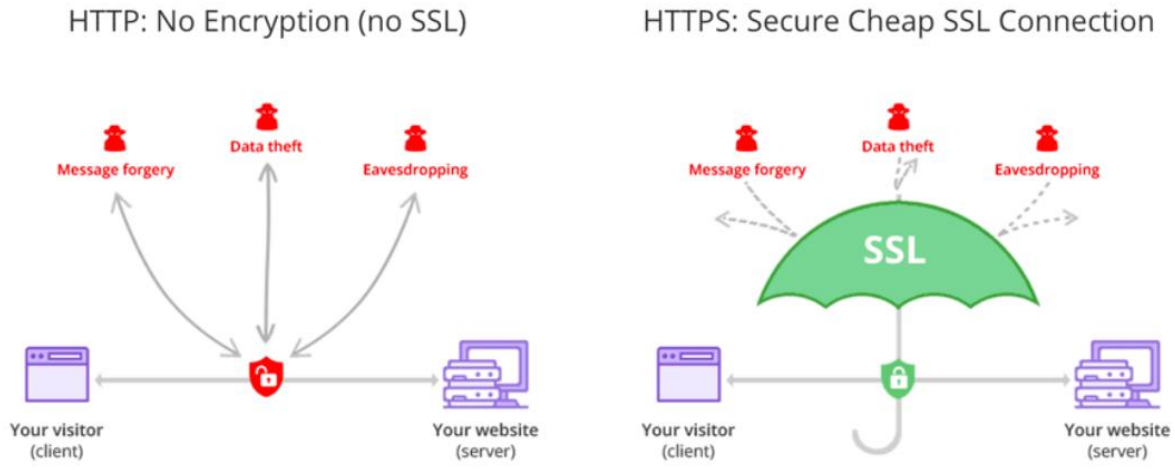
1. SSL/TLS Nedir?

Secure Sockets Layer'ın kısaltılmışı olan SSL'in Türkçe anlamı Güvenli Giriş Katmanı'dır. Netscape tarafından geliştirilmiştir. SSL protokolünün amacı istemci ile sunucu arasındaki bağlantıların güvenliğini sağlamaktır. Bu bağlantının şifreli ve kimliği doğrulanmış bir bağlantı olmasına olanak tanır. İnternet'teki istemci ile sunucu arasında kurulan iletişim şifreli şekilde yapıldığı için gizlilik ve veri bütünlüğü korunur. Kısaca bir şifreleme protokolü olan SSL çoğu web sunucusu ve tarayıcı tarafından desteklenmektedir. İnternette iletişim güvenliğinin dışında ağ taşıma katmanında bulunan uygulamalar için de kimlik doğrulama ve şifreleme amacıyla kullanılan bir protokoldür. SSL ile TCP/IP ağı üzerinde sunucu ve istemci arasında güvenli bir bağlantı kurulabilmesi için public key ve private key kullanılan şifreleme yöntemleri veya diğer şifreleme yöntemleri kullanılmaktadır. Bir anahtar bir veriyi kilitlediğinde bu veriyi yalnızca diğer anahtar açabilir. Yaratılan anahtarlardan sunucuda kalana private key, iletişime geçilmek istenen kişiye gönderilene ise public key adı verilir. İletişime geçmek isteyen kişi public key'i kullanarak bir mesaj gönderir. Gönderilen mesajın aktarım esnasında başka biri tarafından ulaşılması ihtimalinde mesajın çözülebilmesi için private key gerekecektir. Birçok soruna ve zafiyete sahip olduğu için 2015 yılından itibaren kullanımı IETF (İnternet Mühendisliği Görev Gücü - Internet Engineering Task Force) tarafından önerilmemeye başlanmıştır [1,2].

Transport Layer Security'nin kısaltılmışı olan TSL'in Türkçe anlamı Taşıma Katmanı Güvenliği'dir. SSL'in iyileştirilmiş ve güncelleştirilmiş bir halidir. SSL'de olduğu gibi bir iletişimdeki verileri üçüncü şahıslardan saklayarak veri gizliliğini, verilerin kurcalanmayacağını veya sahte olmayacağını doğrulayarak veri bütünlüğünü korumayı ve iletişim kuran tarafların belirtilen taraflar olduğunu kesinleştiren kimlik doğrulamayı sağlayan bir güvenlik protokolüdür. Şifreli iletişim sağlar. E-posta, mesajlaşma ve VoIP gibi iletişimleri de şifrelemektir. Kullanımı IETF tarafından önerilmiştir [3].

Şekil 1: SSL/TLS Sertifikası Olmayan Bir Web Sitesi İle Olan Bir Web Sitesi [4]

HTTP protokolü şifrelemeden yoksun bir protokoldür. Böylelikle saldırganlar bir web sitesine girilen kredi kartı numarası, adres gibi önemli bilgilere kolaylıkla erişebilir. Bu nedenle de HTTP savunmasız bir protokoldür. HTTP Secure olarak adlandırılan HTTPS daha HTTP'nin güvenli bir uzantısı olup iletişimin SSL/TLS kullanılarak şifrelendiğini belirtir. Web sitelerine ait adreslerde bulunan "s" o sitenin SSL veya TLS kullandığını belirtir. Bunun dışında adres çubuğunda bir kilit ikonu yer almaktadır. Böylelikle kullanıcı bilgilerinin saldırganlara karşı güvence altına alındığı belirtilir. Veri ihlalleri bu sayede korunabilir.



Şekil 2: HTTP ve HTTPS Farkı [4]

1.2. SSL/TLS Tarihçesi

1.2.1 SSL'in Tarihi

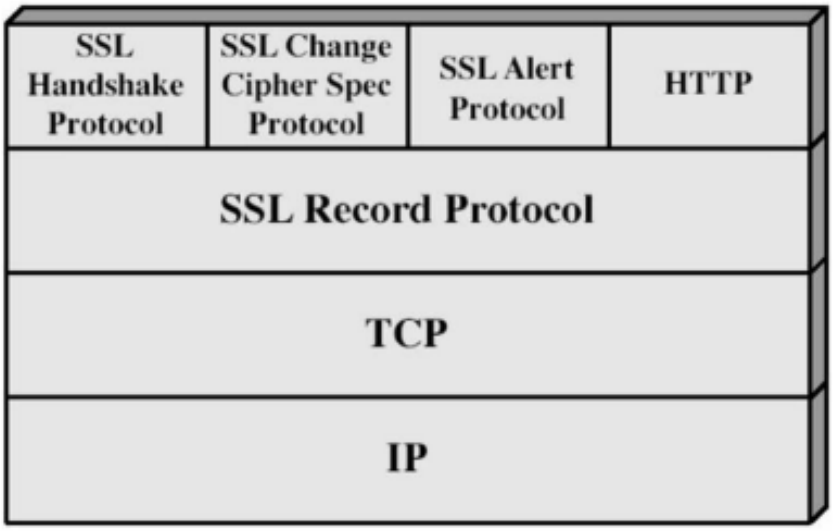
Aktarım güvenliği amacıyla iletişimleri şifrelemek için ortaya çıkan bu protokol ilk olarak Netscape tarafından 1994 yılında geliştirilmiştir. Fakat ciddi güvenlik sorunlarına sahip olan Versiyon 1.0 piyasaya sürülmemiştir. Buradaki sorunlara örnek olarak saldırganların kullanıcılara ait metin mesajlarını değiştirebilmesine olanak tanıyan bir açıklık verilebilir. Daha sonrasında 1995 yılında yine Netscape tarafından Versiyon 2.0 geliştirilmiş ve piyasaya sürülmüştür. Bu sürüm SSL'in ilk resmi kullanılabilir sürümü kabul edilir. Fakat bu sürümde de güvenlik açıklıklarına rastlanılmıştır. Bu sürümde bir kriptografik özet fonksiyonu olan ve birçok güvenlik açığına sahip olan MD5'in kimlik doğrulaması için kullanımı ya da Man-In-The-Middle saldırılarına karşı zayıflık oluşturan yani bu saldırıların tespitini engelleyen açılış el sıkışması veya mesaj kapanışı için korumaya sahip olmaması güvenlik sorunlarına örnek olarak verilebilir. Bu sorunların önüne geçmek amacıyla 1996 yılında SSL 3.0 tanıtılmıştır. 2011 yılında SSL 2.0, 2015 yılında ise SSL 3.0 kullanımdan kaldırılmıştır. SSL 3.0'ın kaldırılma nedeni ise POODLE güvenlik açığına karşı savunmasız olmasıdır. Bu açığı Google ekiplerinden biri bulmuştur. POODLE, Padding Oracle On Downgraded Legacy Encryption'ın kısaltılmış halidir. Saldırganların bu zafiyetten yararlanması durumunda sunucu-istemci arasındaki şifreli iletişim byte byte ortaya çıkabilir. Bu saldırının meydana gelebilmesi için sistemlerin SSL 3.0'ı desteklemesi gerekir. Bu saldırıyla birlikte SSL 3.0'da güvensiz olmuştur. Ek olarak bu güvenlik açığı bulunmadan önce de SSL BEAST ve BREACH gibi bazı zafiyetlere sahipti. [5,6].

1.2.2 TLS'in Tarihi

SSL 3.0'da bulunan güvenlik açıklıklarının ardından 1999 yılında TLS 1.0 geliştirilmiştir. SSL protokolünün güvenlik açısından iyileştirilmiş ve güncelleştirilmiş bir hali olan TLS 1.0'daki değişiklikler ile bu protokol SSL 3.0 ile çalışamayacak hale gelmiştir. Daha sonrasında 2006 yılında TLS 1.1 geliştirilmiştir. Bu sürümdeki değişikliklere örnek olarak şifreli blok zincir saldırılarına karşı eklenen korumalar verilebilir. Bu sürümün ardından 2008 yılında TLS 1.1'i temel alan TLS 1.2 ortaya çıkmıştır. Önceki sürümden farklı olarak bu sürümde MD5-SHA-1 kombinasyonu SHA-256 ile değiştirilmiştir. Daha sonrasında 2018 yılında TLS'in son sürümü olan TLS 1.3 geliştirilmiştir. Bu sürüm TLS 1.2'den daha hızlı ve güvenlidir. Önceki sürümünden farkları için önceki sürümlerde bulunan fakat güncel ya da güvenli olmayan bazı özelliklerin kaldırılması, MD5 ve SHA-224 fonksiyonlarının bu sürümde desteklenmemesi,

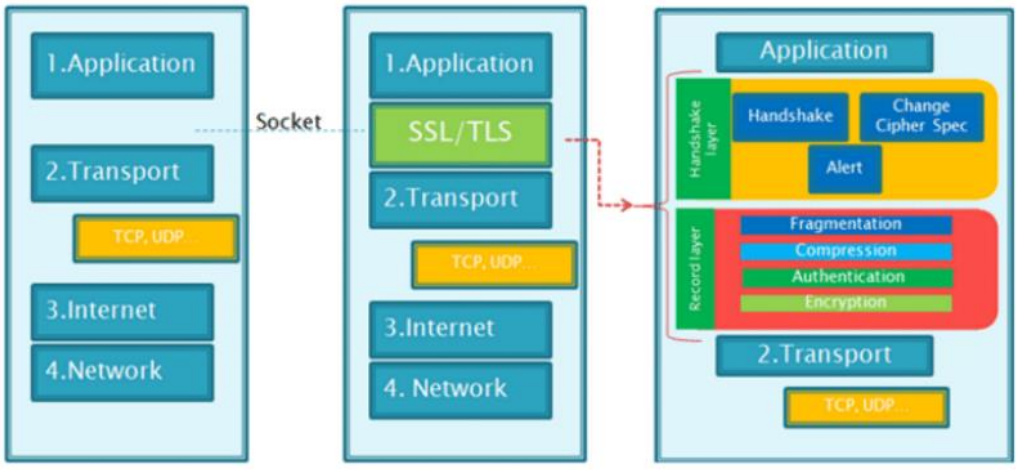
cipher suite'lerden anahtar anlama ve kimlik doğrulama algoritmalarının ayrılması gibi örnekler verilebilir. Günümüzde kullanılabilir olan TLS protokolleri TLS 1.2 ve TLS 1.3'tür [6,7].

1.3. SSL/TLS Yapısı



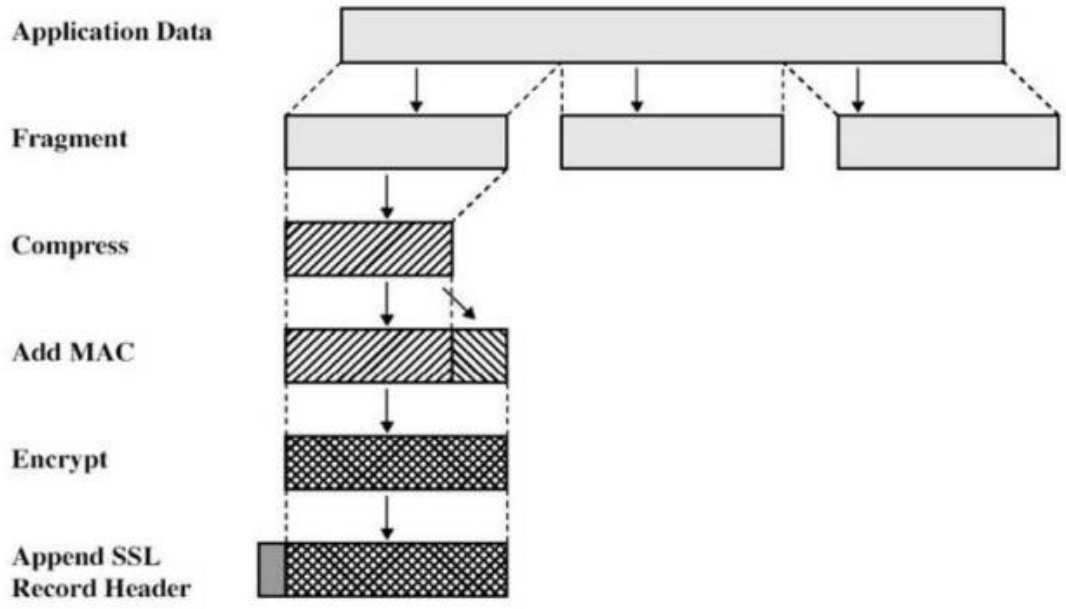
Şekil 3: SSL Protokol Yığını [8]

Şekil 3 ve Şekil 4'te SSL/TLS protokolünün yapısı yer almaktadır. Görüldüğü üzere SSL/TLS, TCP'nin üzerine tasarlanmıştır. SSL/TLS protokolü uygulama katmanı ile taşıma katmanı arasındadır. Şekillerdeki gibi SSL/TLS protokolü iki protokol katmanıdır ve biri doğrudan TCP'yi kullanmaktadır. Doğrudan kullanan katmana SSL Kayıt Protokolü denir. Bu katman üzerindeki protokollere güvenlik sağlamaktadır. Kayıt katmanı dört protokolü desteklemektedir. Bunlar SSL Kayıt Protokolü (SSL Record Protocol), SSL El Sıkışma Protokolü (SSL Handshake Protocol), Change - Cipher Protokolü (Change Cipher Spec Protocol) ve Uyarı Protokolüdür (Alert Protocol) [8,9].



Şekil 4: SSL/TLS Protokolü Yapısı [10]

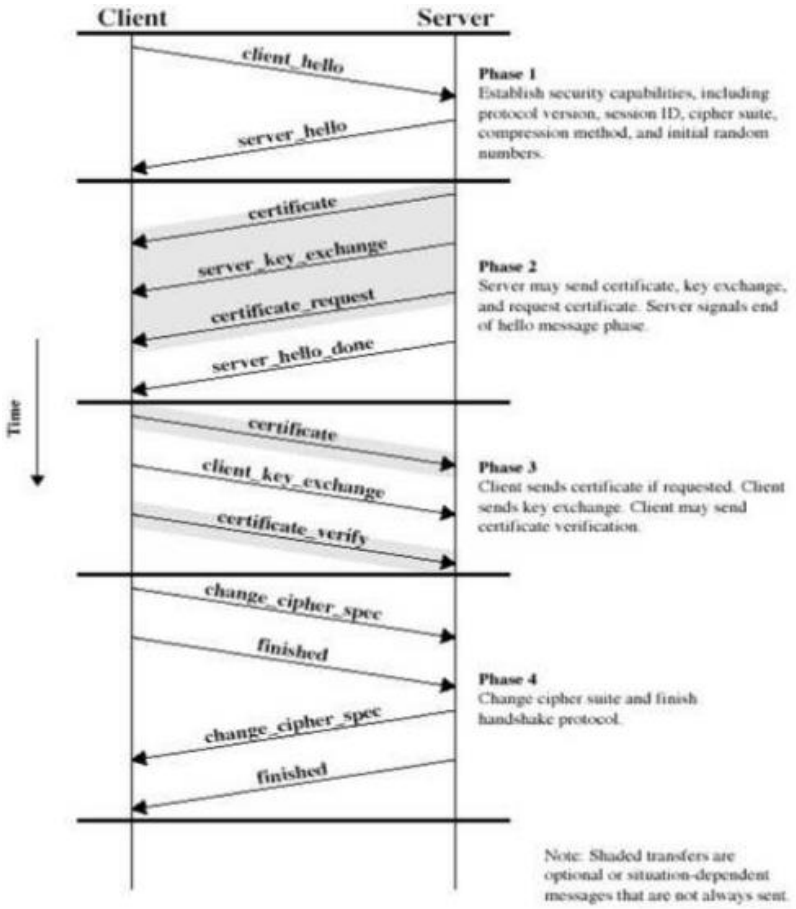
1. **SSL Kayıt Protokolü (SSL Record Protocol):** Bu protokol SSL bağlantısına gizlilik ve mesaj bütünlüğü -MAC kullanılmasıyla- sağlamaktadır. Bu protokolde Şekil 5'te görüldüğü üzere ilk olarak veriler parçalara ayrılır. Daha sonraki adımda bu parçalar sıkıştırılır. Sıkıştırıldıktan sonra sıkıştırılmış veriler üzerinden SHA (Secure Hash Protocol) ve MD5 (Message Digest) gibi algoritmaların kullanılmasıyla oluşturulan şifreli MAC (Message Authentication Code) sıkıştırılan bu parçaya eklenir. Daha sonrasında sıkıştırılmış veri ile MAC şifrelenir. Burada bazı şifreleme algoritmaları kullanılabilir. Son olarak SSL başlığı eklenir.



Şekil 5: SSL Kayıt Protokolü İşlemi

2. **SSL El Sıkışma Protokolü (SSL Handshake Protocol):** Bu protokol oturum oluşturmak amacıyla kullanılmaktadır. İstemci ile sunucu arasındaki doğrulamayı sağlar. Bunu yaparken istemci ve sunucu birbirlerine bir dizi mesaj gönderir. Şekil 6'da görüldüğü üzere dört aşamadan oluşan bu protokolde ilk olarak istemci de sunucu da birbirlerine hello paketlerini gönderirler. İkinci aşamada ise sunucu, sertifikasını sunucu anahtar değişimini (Server-key-exchange) gönderir. En son sunucu Server-hello-end paketini gönderir. Böylelikle aşama 2 son bulur. Üçüncü aşamada istemci sertifikasını istemci anahtar değişimini (Client-key-exchange) gönderir. Böylelikle sunucuya cevap

vermiş olur. Son aşamada ise Change-cipher paketi oluşur. Güvenli bağlantı oluşturulmuştur ve istemci ve sunucu verileri gönderilebilir.



Şekil 6: SSL El Sıkışma protokolü çalışması

3. **Change - Cipher Protokolü (Change Cipher Spec Protocol):** Bu protokol bir mesajdan oluşur. Bu mesaj bir bayt boyutundadır ve bir değeri almaktadır. SSL kaydı, El Sıkışma Protokolü tamamlanmadıkça bekleme durumunda kalacaktır. Tamamlandıktan sonra ise bekleme durumu mevcut durum olur. Bu aşamada bekleme durumunu kullanılacak paketi güncelleyecek olan mevcut duruma kopyalanmasını sağlamak amacıyla bu protokol kullanılmaktadır.
4. **Uyarı Protokolü (Alert Protocol):** Bu protokol SSL ile ilgili uyarıları iletmek amacıyla kullanılmaktadır. Her mesaj iki byte içerir. Bu iki byte'ın ilki, uyarı (warning) ve ölümcül hata (fatal error) şeklinde ikiye ayrılmıştır. Uyarı değeri, gönderici ile alıcı arasındaki bağlantıyı etkilemez. Ölümcül hata değerinde ise gönderici ve alıcı arasındaki bağlantı anında kesilir. Diğer byte belirli bir uyarıyı gösteren bir kodu içerir.

1.4 SSL/TLS Sertifikası

SSL/TLS protokolü X.509 standardı ile çalışır. Bu standart dijital sertifika formatını belirtir. Dijital sertifikalar dijital bir belge olup kriptografik anahtar çiftlerini web siteleri ile kişiler ya da kurumlar gibi kimliklerle ilişkilendirir ve doğrulamaya yarar. Bu anahtar çiftleri bir public key bir de private key'den oluşur. Anahtarlar arasında olan matematiksel ilişki nedeniyle bir public key ile şifrelenen veri sadece private key ile çözülebilir. Güvende tutulan private key ile sahipleri dijital belgeleri imzalayabilir [11].

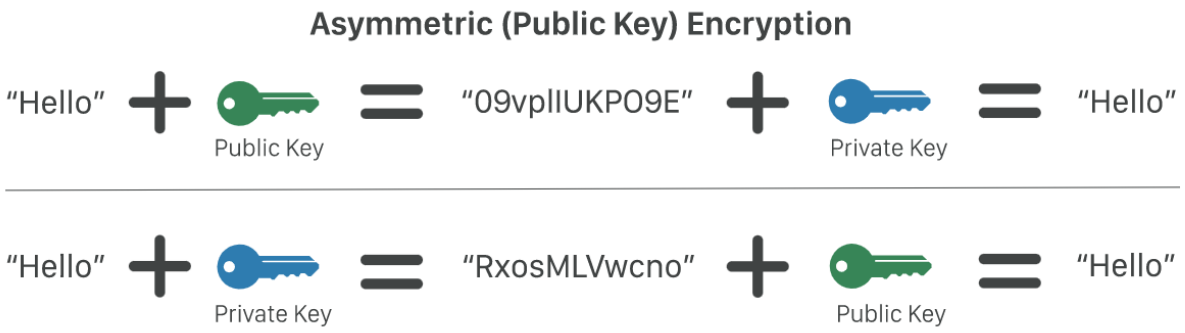
Dijital sertifikaların içeriği sertifikanın verildiği kişi/kuruluş/cihaz, tüm sertifika verilerinin ve imzasının bir özeti olan parmak izi, kullanılan SSL/TLS sürümü, yayınlayan sertifika yetkilisinin adı ve dijital imzası, sertifikanın verildiği ve sona erdiği tarihler, public – private key gibi birçok bilgiden oluşur [1].

Kullanıcılara ait verilerin güvence altına alınması amacıyla bir web sitesinin kimliğini doğrulamak, saldırganların bir web sitesinin sahte bir sürümünü oluşturmasını engellemek ve kullanıcılara sitenin güvenilir bir site olduğunu belirtmek amacıyla web siteleri SSL sertifikalarına sahip olmalıdır. Bu sertifika ile birlikte kullanıcılara ait oturum açma bilgileri, kredi kartı veya banka bilgileri gibi finansal bilgiler, kullanıcıya ait ad, soyad, adres, doğum tarihi, telefon numarası gibi bilgiler, yasal belgeler, tıbbi kayıtlar çevrimiçi yapılan işlemlerde güvence altına alınır. SSL sertifikalarının doğrulama seviyeleri farklı olabilir. SSL sertifikalarına örnek olarak Genişletilmiş Doğrulama sertifikaları (EV SSL), Kuruluş Doğrulama sertifikaları (OV SSL), Etki Alanı Doğrulama sertifikaları (DV SSL), Wildcard SSL sertifikaları, Çok Etki Alanlı SSL sertifikaları (MDC) ve Birleşik İletişim Sertifikaları (UCC) verilebilir. SSL sertifikası güvenilir bir sertifika yetkilisi (Certificate Authority - CA) tarafından imzalanmaktadır. Verilen sertifikaların belirli bir geçerlilik süresi vardır. Bu süre en fazla 27 ay olabilir. Sertifikalar geçerlilik süresi dolmadan yenilenmelidir. Dolmasıyla web sitesi erişilemez hale gelir. Kullanıcı erişmeye kalkıştığında "Bu site güvenli değil" benzeri bir mesaj ile karşılaşır. Her ne kadar bu mesaj ardından o siteye giriş önerilmese bile kullanıcıya devam etme seçeneği de sunulmuştur. Kullanıcı bu mesaja rağmen web sitesine girerse bazı siber risklerle karşı karşıya kalabilir [12].

1.5 SSL/TLS Çalışma Prensibi

SSL/TLS protokolünde açık anahtarlı şifreleme teknolojisi kullanılmaktadır. Bu teknolojide iletişim kuran tarafların her birinde bir çift anahtar vardır ve şifreleme - deşifreleme yöntemleri

için farklı anahtarlar bulunmaktadır. Bu yöntemde asimetrik anahtar algoritmaları kullanıldığı için yöntem asimetrik şifreleme olarak da geçmektedir [13].



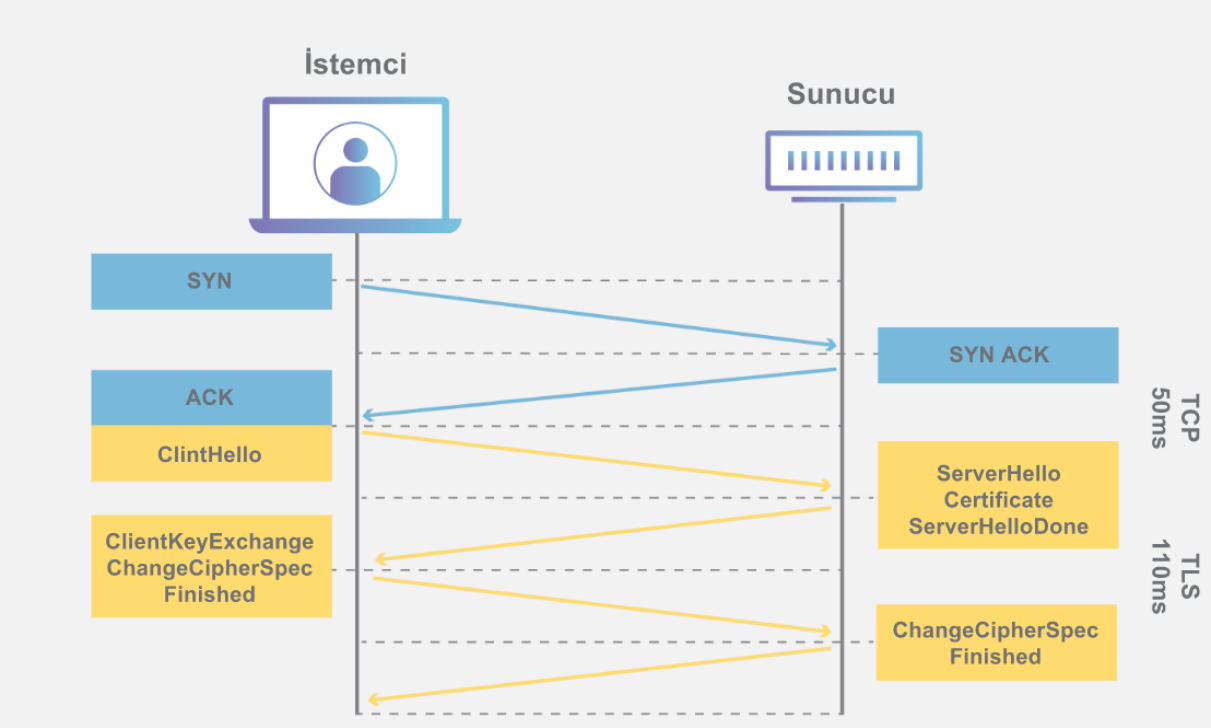
Şekil 7: Asimetrik Şifreleme [14]

İstemci sunucuyla bağlantı kurmak istedikten sonra sunucu istemciye sertifika ve public key (açık anahtar) göndermektedir. İnternet tarayıcısı istemcinin gönderdiği bilgileri kontrol etmek amacıyla gelen sertifikanın güvenilirliğini denetler. Sertifika, sertifika otoritesinen (Certificate Authority - CA) geçerse doğrulanmış olur ve geçerli olduğu anlaşılır. Public key'e güvenilebileceği anlaşılır ve tarayıcı simetrik bir anahtar üretir. Public key ile üretilen bu anahtar şifrelenerek sunucuya gönderilir. Sunucu aldığı public key ile şifrelenmiş mesajı kendisindeki public key ile dener. Mesajı doğruladıktan sonra ise kendisinde bulunan private key'i kullanarak simetrik anahtar elde eder. Bundan sonra sunucudan istemciye aktarılacak olan verilerde elde edilen bu simetrik anahtar kullanılacaktır. İstemci ise sunucunun ulaştırdığı verileri bu simetrik anahtarı kullanarak çözüp tarayıcıda istediği tüm bilgileri görüntüleyebilir [15].

SSL/TLS protokolü kullanıcılara ait bilgilerin üçüncü kişiler tarafından gizli bir şekilde ele geçirilmesini ve değiştirilmesini önler. İstemci sunucuyla bağlantı kurmak istediğinde SSL/TLS bağlantısına dair isteğini belirtmelidir. Bunun için bulunan yollardan biri SSL/TLS uzantıları için farklı port numaralarının kullanılmasıdır. Örnek olarak HTTP ile bir uzantısı olan HTTPS'in farklı port numaraları vardır. HTTP için 80. port ayrılmışken HTTPS için 443. port ayrılmıştır. Diğer yolda ise sıradan bir port kullanılmaktadır. Bu durumda SSL/TLS protokolünün istemciler için özelleştirilen bir mekanizması kullanılır. İstemci bu mekanizmayla sunucunun bağlantıyı SSL/TLS protokolüne aktarması gerektiğini gösterir [15].

1.6 SSL/TLS Handshake

İstemci ve sunucu arasında SSL/TLS protokolü kullanılarak yapılan bir iletişim başladıktan sonra bağlantı kurmak için ilk yapılan işlem SSL/TLS Handshake ya da SSL/TLS El Sıkışması olarak adlandırılır. Bu işlem esnasında istemci ve sunucu birbirlerini tanımak ve doğrulamak, kullanılacak şifreleme algoritmasını oluşturmak, oturum anahtarlarını belirlemek için birbirlerine bir dizi mesaj gönderirler. Kullanılan SSL/TLS sürümü, kullanılacak şifre paketleri belirlenip sunucunun public key'inin ve sunucunun kimliğinin doğrulanması yapılır. SSL/TLS el sıkışmasındaki adımlar kullanılan anahtar değişim algoritması türü ve istemci – sunucu tarafından desteklenen şifre paketlerine bağlı olarak değişmektedir. RSA en çok kullanıla algoritmalardan biri RSA'dır. İlk adımda istemci sunucuya bir "hello" mesajı gönderir. Böylelikle el sıkışma başlamış olur. Mesaj içerisinde istemcinin desteklediği TLS sürümü, şifre paketleri, "client random" olarak bilinen bir diziyi bulundurur. Ardından ikinci adımda sunucu istemcinin "hello" mesajını bir "hello" mesajı göndererek yanıtlar. Bu mesaj içerisinde de sunucuya ait SSL sertifikası, seçilen şifre paketi, "server random" olarak bilinen bir diziyi bulundurur. Üçüncü adımda kimlik doğrulama yapılır. İstemci sunucunun SSL sertifikasını doğrulama işlemini gerçekleştirir. Bunu sertifikayı veren yetkili ile gerçekleştirir. Doğrulama gerçekleştiğinde istemci sunucunun sahte olmadığını, alan adının gerçek sahibinin o olduğunu doğrulayabilmiş olur. Gerçekleşmezse istemci bilgilendirilir ve ardından bağlantı kesilir. Bir sonraki adımda istemci public key ile şifrelenmiş rastgele bir byte dizisi gönderir. Bu dizi yalnızca sunucuda bulunan private key ile çözülebilmektedir. Sunucu kendi public key'i denedikten sonra olumlu sonuca varırsa beşinci adıma geçilir. İstemci doğrulanamazsa oturum bitirilir. Beşinci adımda ise gönderilen bu veriyi sunucu private key kullanarak deşifre eder. Altıncı adımda ise istemci ve sunucu paylaşılan veri ile simetrik oturum anahtarları oluşturup aynı sonuçlara varmaları beklenir. Bunun ardında yedinci adımda istemci hazır olduğunu belirten oturum anahtarıyla şifrelenen bir "finished" mesajı gönderir. Sekizinci adımda ise sunucu oturum anahtarıyla şifrelenen bir "finished" mesajı gönderir. Son olarak dokuzuncu adımda ise el sıkışma işlemi tamamlanmış olur. İletişim oturum anahtarlarıyla devam eder [16].



Şekil 8: SSL/TLS El Sıkışması [16]

1.7 SSL/TLS Hedefleri

SSL/TLS protokolünün amaçları aşağıda genel olarak yedi başlık altında açıklanmıştır [10].

- **Gizlilik:** Kullanıcılara ait şifreler, finansal bilgiler gibi veriler bir ağ veya İnternet üzerinden iletilirken gizliliği sağlanmalıdır. Üçüncü şahıslar bu bilgileri ele geçirememelidir. SSL/TLS protokolü ile bu gizlilik şifreleme yapılarak sağlanmaktadır.
- **Bütünlük:** Verilerin birleşik kalıp kurcalanmamalıdır. Üçüncü bir şahıs yani bir saldırgan bu verilerin iletileceği noktayı ya da verinin içeriğini değiştirememelidir.
- **Kimlik Doğrulama:** Kuruluşların sistemlerine erişen kişilerin kimliğinin doğrulaması gerekmektedir.
- **Kriptografik Güvenlik:** İstemci ile sunucu arası güvenli bir bağlantı kurmak amacıyla SSL/TLS protokolü kullanılmalıdır.
- **Birlikte Çalışabilirlik:** Bağımsız programcılar SSL/TLS protokolü kullanan başarılı bir şekilde kriptografik parametre değiş tokuşu yapabilen programlar geliştirebilmelidir.
- **Genişletilebilirlik:** SSL/TLS protokolünde yeni public key ve toplu şifreleme yöntemlerinin içerildiği geniş bir yapı sağlanmalıdır. Böylelikle yeni bir protokol oluşturulması ve uygulama ihtiyacını önlenir.

- **Göreceli Verimlilik:** Kriptografik işlemler çok yüksek miktarda CPU kullanır. Bu nedenle sıfırdan kurulan bağlantı sayısı azaltılıp isteğe bağlı oturumların önbelleğe alınması gerekmektedir.

1.8 SSL/TLS Uygulamaları

- **Web Siteleri:** SSL/TLS bir web sayfası ile tarayıcı arasındaki iletişimi HTTPS ile güvenli hale getirir. Temel kullanım amaçlarından birisi budur. Böylelikle kullanıcı verileri güvence altına alınmış olur. Web sitelerinde Ekim 2021'e göre SSL 2.0 ve SSL 3.0 güvensiz kabul edilmektedir ve web sitesi destekleri çok düşüktür. TLS 1.0 ve TLS 1.1'in web sitesi destekleri SSL'e göre yüksek olmasına rağmen kullanımdan kaldırılmıştır. TLS 1.2 ise çok yüksek web sitesi desteğine sahip olup güvenliği şifre gibi bazı durumlara bağlıdır. TLS 1.3 ise güvenli kabul edilmektedir ve web sitesi desteği ise %49.7'dir [6].
- **Web Tarayıcıları:** 2016 yılı itibariyle tüm büyük web tarayıcılarının son sürümleri TLS 1.0, 1.1, ve 1.2 versiyonlarını desteklemektedir. Bunun yanında aktif edilmiş halde sunar. Fakat bazı bilinen saldırılara karşı hafifletmeler henüz yeterli değildir. POODLE saldırısında bazı tarayıcılar SSL 3.0'a dönüşü engellese bile bunun yalnızca istemci değil sunucu tarafında da desteklenmesi gerekmektedir. Google Chrome'da, Mozilla Firefox'da ve Opera'da SSL 3.0 desteği kaldırılmıştır. RC4 saldırılarına karşı azaltmada ise Google Chrome'da, Mozilla Firefox'da ve Opera'da RC4 devre dışı bırakılmıştır. FREAK saldırısı için ise Android 4.0 ve daha eski sürüme sahip cihazlarda bulunan Android tarayıcılar hala bu saldırıya karşı savunmasızdır. Google Chrome ve Opera (mobil) , Safari (mobil ve masaüstü) bu saldırı için azaltmalara sahiptir. Mozilla Firefox ise tüm platformlarda FREAK saldırısından etkilenmemektedir [6].
- **Kütüphaneler:** Sıklıkla kullanılan açık kaynaklı SSL/TLS kütüphanelerine örnek olarak Botan, cryptlib, Delphi, GnuTLS, Java Secure Socket Extension, LibreSSL, MatrixSSL, mbed TLS, Network Security Services, OpenSSL, SChannel, Secure Transport ve wolfSSL verilebilir [6].
- **Diğer Kullanımları:** SMTP protokolü SSL/TLS ile korunabilir. SIP protokolü uygulamalarında koruma için kullanılır. SIP tabanlı uygulamalar ve VoIP için kimlik doğrulama ve şifreleme sağlayabilir. Bunun dışında SSL/TLS kullanılarak VPN oluşturulabilir [6].

KAYNAKÇA

1. Cobb, M. Loshin, P. (2021). SSL (secure sockets layer) https://www.techtarget.com/searchsecurity/definition/Secure-Sockets-Layer-SSL
2. SSL Nedir, Nasıl Çalışır? (t.y.) https://www.hosting.com.tr/bilgi-bankasi/ssl-nedir-nasil-calisir/
3. What is TLS (Transport Layer Security)? (t.y.) https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/
4. M. Gürkan, (2022). HTTPS, TLS ve SSL Nedir? Ne İşe Yararlar? https://www.hostinger.web.tr/rehberler/https-tls-ve-ssl-nedir-ne-ise-yararlar
5. THE EVOLUTION OF SSL AND TLS. (2015). https://www.digicert.com/blog/evolution-of-ssl
6. Transport Layer Security. (2022). https://en.wikipedia.org/wiki/Transport_Layer_Security
7. Yackel, R. (2020). What is SSL? Understanding the History of SSL and How it Works https://www.keyfactor.com/blog/what-is-ssl/
8. Mukhopadhyay, S. (t.y.) THE SECURE SOCKETS LAYER (SSL) http://www.facweb.iitkgp.ac.in/~sourav/lecture_note10.pdf
9. Secure Socket Layer (SSL). (2021). https://www.geeksforgeeks.org/secure-socket-layer-ssl/
10. Elnaggar, A. (t.y.) Secure Socket Layer https://www.researchgate.net/publication/283297122_Secure_Socket_Layer
11. What is SSL? (2021). https://www.ssl.com/faqs/faq-what-is-ssl/
12. SSL sertifikası nedir? – Tanım ve Açıklama. (t.y.) https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-ssl-certificate
13. Açık anahtarlı şifreleme. (2022). Vikipedi https://tr.wikipedia.org/wiki/A%C3%A7%C4%B1k_anahtarl%C4%B1_%C5%9Fifreleme
14. How does SSL work? | SSL certificates and TLS (t.y.) https://www.cloudflare.com/learning/ssl/how-does-ssl-work/#:~:text=Secure%20communication%20begins%20with%20a,communications%20after%20the%20TLS%20handshake

15. Transport Layer Security (TLS) Nedir? (2021). https://www.natro.com/blog/transport-layer-security-tls-nedir/
16. What happens in a TLS handshake? | SSL handshake. (t.y.) https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/