



BİLGİSAYAR AĞLARI GÜVENLİK PROTOKOLLERİ (*UYGULAMA VE ULAŞIM KATMANLARI*)

İÇERİK;

- 1. Bilişimde Güvenlik Politikaları
- 2. Protokol Nedir?
- 3. Protokol Türleri
- 4. OSI Modeli ve Protokol Kümeleri
 - 4.1 Uygulama (Application) Güvenlik Protokolleri
 - 4.1.1 PGP (Pretty Good Privacy)
 - 4.1.2 S/MIME(Secure/Multipurpose Internet Mail Extension)
 - 4.1.3 S-HTTP
 - 4.1.4 HTTPS(Secure Hypertext Transfer Protocol)
 - 4.1.5 SET(Secure Electronic Transactions)
 - 4.1.6 KERBEROS



İÇERİK;

- 4.2 Ulaşım (Transport) Güvenlik Protokolleri
 - 4.2.1 SSH (Secure Shell/Güvenlik Kabuk)
 - 4.2.2 SSL (Secure Socket Layer-Güvenli Yuva Kağıdı)
 - 4.2.3 PCT (Private Communication Technology-Kişisel İletişim Teknolojisi)
 - 4.2.4 TLS (Transport Layer Security-İletim Katmanı Güvenliği)
 - 4.2.5 Sonuçlar



1. BİLİŞİMDE GÜVENLİK POLİTİKALARI

- Bilginin ve kaynakların paylaşılması gereksinimi sonucunda kurumlar, bilgisayarlarını çeşitli yollardan birbirine bağlayarak kendi bilgisayar ağlarını kurmuşlar ve sonra dış dünyayla iletişim kurabilmek için bilgisayar ağlarını İnternet'e uyarlamışlardır.
- İnternet yasalarla denetlenemeyen bir sanal dünyadır. Bu sanal dünyada sadece yapılan saldırılarla değil, aynı zamanda kullanıcıların bilinçsizce yaptıkları hatalar nedeniyle birçok bilgi başka kişilerin eline geçmekte veya içeriği değiştirilmektedir.



BİLİŞİMDE GÜVENLİK POLİTİKALARI

- Kurumlarda oluşan kayıplar maddi olabileceği gibi güven yitirme gibi manevi zararlar da olabilmektedir.
- Bu tür durumlarla başa çıkabilmek için bazı kuralların belirlenmesi gerekmektedir.



2. PROTOKOL NEDİR?



- Ağ üzerinde iki bilgisayarın karşılıklı veri aktarabilmesi ve ortak süreçler yürütebilmesi için bilgisayarların karşılıklı çalışabilme yeteneğinin olması gerekir. Birlikte çalışabilme, verici ve alıcı arasında kullanılacak işaretler, veri formatları ve verinin değerlendirme yöntemi üzerinde anlaşma ile mümkün olur. Bunu sağlayan kurallar dizisi de protokol olarak adlandırılır.



PROTOKOL NEDİR?

- Çok sayıda protokol vardır. Ancak her birinin değişik amaçları vardır. OSI modeline göre veri iletiminde birçok protokol birlikte çalışır. Bu bilesime protokol kümesi (protocol stack) denir. Böylece bir protokol kümesinde farklı protokoller bulunabilir.
- OSI katmanı protokolün fonksiyonunu da belirler. Örneğin bir protokol fiziksel katmanda çalışıyorsa onun görevi verinin kablo ile iki network kartı arasında iletimidir.



3. PROTOKOL TÜRLERİ

- Protokollerin türleri değişik şekillerde tanımlanabilir:
- **Açık protokoller;** TCP/IP gibi herhangi bir firma tarafından değil de geniş toplulukların oluşturdukları komiteler tarafından yönetilirler. Bu protokoller diğer protokollerle uyumlu çalışırlar.
- **Firma protokolleri;** Bir firma tarafından özellikle kendi işletim sistemi ve ürünleri için tasarlanmış protokollerdir. Örneğin Novell'in IPX/SXP ve Banyan firmasının protokolleri bu sınıfa girer.



4. OSI MODELİ VE PROTOKOL KÜMELERİ

- OSI modeli, katmanlı bir iletişim modelini kullanmaktadır. Gerçekte katmanlara ayrılmış bir dizi protokol networkü gerçekleştirir.
- Katmanlara ayrılmış protokollere ise protokol kümesi denir. Küme içindeki protokoller iletişimdeki paketleme, gönderme ve alma gibi işlemleri yerine getirirler.



OSI MODELİ VE PROTOKOL KÜMELERİ

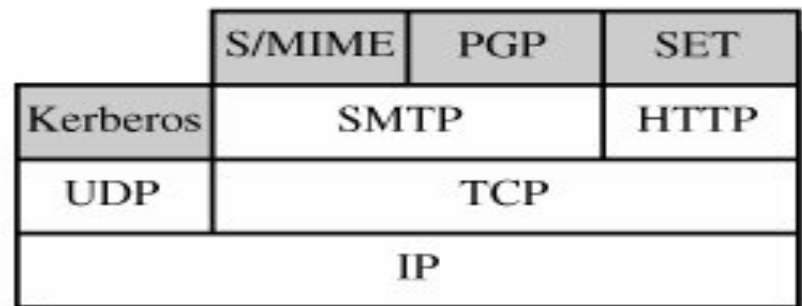
- Protokollerin görevi iki bilgisayar arasındaki iletişim kurallarını düzenlemek ve verilerin gönderilmesini sağlamaktır.
- Bu anlamda OSI modeli içindeki yedi katmandaki görevleri yerine getirmek için gereken protokoller katmanı üç bölümden oluşur:

- - Application (uygulama)
- - Transport (ulaşım)
- - Network



4.1 UYGULAMA (APPLICATION) GÜVENLİK PROTOKOLLERİ

- Application protokolleri OSI Application katmanında çalışır. Bu protokol uygulamadan-uygulamaya verilerin iletimini sağlar.
- Bu alanda yaygın olarak kullanılan güvenlik protokolleri;
- *-PGP*
- *-S/MIME*
- *-S-HTTP*
- *-HTTPS*
- *-SET*
- *-KERBEROS*



(c) Application level



4.1.1 PGP (PRETTY GOOD PRIVACY)



- Kullandığı kript algoritmalarının kuvvetliliği ile dikkati çeken PGP, kendini dijital mahremiyetin korunmasına adanmış bir aktivist olan Phil Zimmermann tarafından geliştirilen ve gayri ticari kullanımı ücretsiz bir e-posta güvenlik yazılımıdır.
- PGP sayesinde e-maillerinizi ve dosyalarınızı 3. gözlerden rahatça uzak tutabilirsiniz. İstemediğiniz kişiler dosyalarınızı e-maillerinizi ele geçirse bile, eğer PGP ile şifrelenmişse bu dosyaların içeriklerine ulaşamazlar.



PGP (PRETTY GOOD PRIVACY)

- PGP melez bir şifreleme kullanır. Geleneksel ve Asimetrik şifrelemenin bir karışımı olan Halka Açık Anahtarla Şifreleme (Public Key Encryption) sistemidir.
- Halka Açık Anahtar sisteminin en büyük avantajı, anahtarların alıcı ve verici arasında değiş tokuşu için güvenli bir kanala ihtiyaç duymamasıdır. Bununla birlikte, bir kez kapatılan veya şifrelenen dosya, ancak ve ancak alıcısının özel anahtarı ile açılabilmekte veya deşifre edilebilmektedir.



PGP (PRETTY GOOD PRIVACY)

- PGP'de;

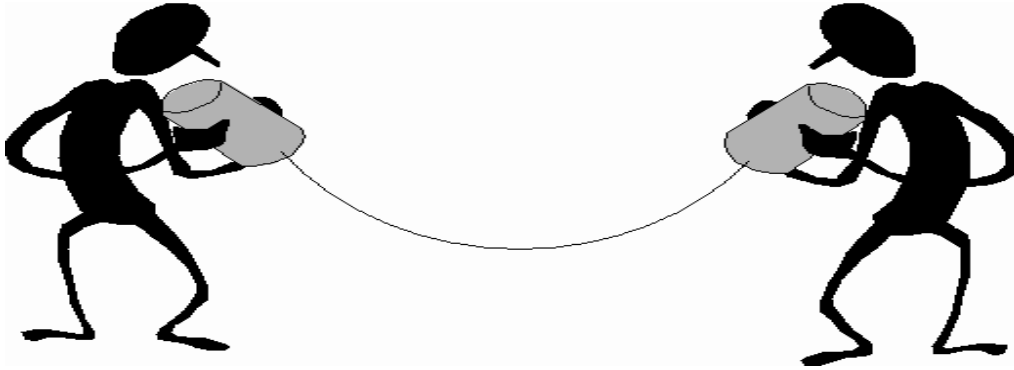


1. E-mail' i alacak kişi (alıcı) gönderecek olana Genel Anahtarını gönderir.
2. E-mail' i gönderecek kişi, (gönderici) alıcının Genel Anahtarını "import" eder.
3. Gönderici yeni e-mailini alıcının genel anahtarı ile şifreler.
4. Alıcı gelen e-maili kendi özel anahtarı ile çözümler.



PGP (PRETTY GOOD PRIVACY)

- PGP ‘nin diğ er bir  zelliđi ise i erdiđi g ven mekanizmalarının karmaşıklığıdır. G venli otorite kavramına karsı  ıkan bir yaklaşımın  r n  olduđu i in, isteyen herkes a ık anahtarları onaylayan bir otorite olabilir. Ancak kullanıcılar g vendiđi kiřileri kendileri se erler.



4.1.2 S/MIME (SECURE/MULTIPURPOSE INTERNET MAIL EXTENSION)

- S/MIME bir e-mail içeriğinin nasıl düzenlenmesi gerektiğini belirleyen, Internet'te güvenli mail yollamak için kullanılan bir protokoldür.
- S/MIME bildiğimiz mail formatına sayısal imza ve şifreleme özelliklerini eklemiştir.
- Bu standartlaştırma işlemi çok farklı e-mail yazılımı kullanan farklı kullanıcıların birbirleriyle iletişimini sağlar. Sertifikanızı kullanarak güvenli e-mail alıp yollayabilmeniz için kullandığınız e-mail yazılımının S/MIME protokolünü desteklemesi gerekir.



S/MIME (SECURE/MULTIPURPOSE INTERNET MAIL EXTENSION)

- RGP, kullandığı kript algoritmalarının güçlü olmasına rağmen karışık bir güvenlik mekanizması içermektedir.
- İsteyen herkes açık anahtarları onaylayan bir otorite olabildiği ve açık anahtarların tutulduğu PGP sunucusu herhangi bir güvenlik sözü vermediği için, kullanıcılar güvendiği sertifikaları kendileri seçerler ve bu da güvenlik konusunda uzman kullanıcılar gerektirir.



S/MIME (SECURE/MULTIPURPOSE INTERNET MAIL EXTENSION)

- S/MIME ise açık anahtarların sahiplerinin doğruluğunu garantileme mekanizması olarak güvenli sertifika otoritelerini (Certification Authority – CA) kullanmaktadır.
- Aslında birer şirket olan bu otoriteler, kişilere ve kurumlara ücret karşılığında dijital kimlik olarak da adlandırılan sertifikalar pazarlamaktadırlar.
- Bu sertifikalar içinde, kullanıcı bilgileri ile beraber sertifika sahibinin açık anahtarı da bulunmaktadır. Sertifikayı dijital olarak imzalayan CA, sertifika içinde var olan bilgilerin doğruluğuna garanti vermektedir.



4.1.3 S-HTTP

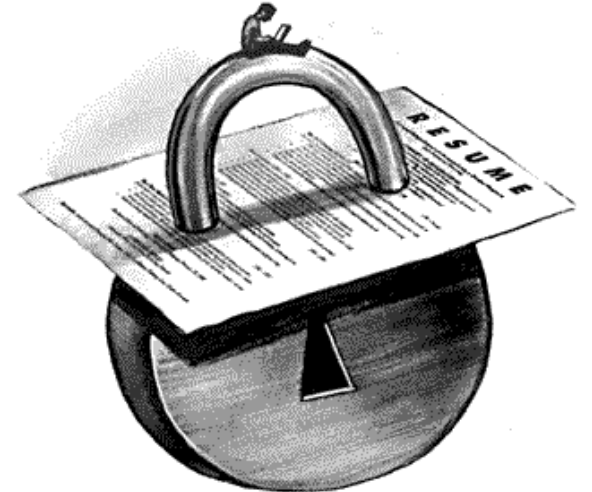


- Enterprise Information Technologies tarafından geliştirilmiş olan, şifreleme ve kullanıcı doğrulama yeteneklerine sahip güvenli HTTP veya S-HTTP olarak bilinen ürün, internet ortamında kullanılan bir diğer şifreleme yaklaşımıdır.
- Tasarlanma amacı gizlilik, kimlik doğrulama, bütünlük, ve inkar edememe (kendisinden başkası olduğunu söyleyememe) olan S-HTTP, aynı zamanda birden çok anahtar-yönetimi mekanizmasını ve şifreleme algoritmasını, taraflar arasındaki aktarımda yer alan seçenek kararlaştırılması yoluyla destekler.



S-HTTP

- Bu şifreleme yaklaşımı, HTTP protokolünün içerisine yerleştirilmiş olduğundan, HTTP protokolünün ürettiği istek ve cevap başlıklarını etkilemekte, ilave alanlar getirmektedir.
- Bu alanlarda aktarılan ek bilgiler; kullanılan şifrelemenin tipi, şifreleme anahtarlarının değişimi için bu anahtarlara ilişkin alanlar, verilere ilişkin olarak hesaplanmış olan özet bilgiyi içeren bir alan içindeki bilgilerdir.



S-HTTP

- Bu şekliyle aslında S-HTTP Temel Kullanıcı Doğrulama mekanizmasına benzer.
- Ancak görüldüğü gibi burada ek olarak şifreleme anahtarları vardır ve doğrulama, dolayısıyla tanıma işlemi karşılıklı olarak yapılmaktadır.



- Ayrıca S-HTTP, kendisini hayata geçirmiş olan belirli yazılımlarla sınırlıdır, ve her bir mesajı ayrı ayrı şifreler.



4.1.4 HTTPS (SECURE HYPERTEXT TRANSFER PROTOCOL)

- HTTPS (Güvenli hiper metin aktarım iletişim kuralı), hiper metin aktarım iletişim kuralının (HTTP) güvenli ağ protokolü ile birleştirilmiş olanıdır.
- Klasik HTTP protokolüne SSL protokolünün eklenmesi ile elde edilir.
- İnternette sunucular ve son kullanıcılar arasında bilgilerin "başkaları tarafından" okunamayacak şekilde nasıl aktarılacağına dair kurallar ve yöntemleri düzenleyen bir sistemdir.



4.1.5 SET(SECURE ELECTRONIC TRANSACTIONS)

- SET (Secure Electronic Transactions-Güvenli Elektronik İşlemler) Visa, Mastercard, Netscape ve Microsoft'un birlikte geliştirdiği bir kriptografik protokoldür.
- Haberleşmeleri kriptolama için kullanılan genel amaçlı SSL'den farklı olarak SET sadece müşteri ile tüccar arasındaki kredi ve "debit" kartları işlemlerini güvenli hale getirmede kullanılır.



SET(SECURE ELECTRONIC TRANSACTIONS)

- Alt seviyede, SET protokolü aşağıdaki ana servisleri sağlar:
- **Kimlik Tanılama;** Kredi kartı işlemlerindeki tarafların kimlik tanılması dijital imzalar ile gerçekleştirilir. Buna müşteri, tüccar, müşterinin kredi kartını sağlayan banka ve tüccarın kontrol hesabı ile ilgilenen banka dahildir.
- **Gizlilik;** İşlemler kriptolandığı için gizlice dinlenemez.



SET(SECURE ELECTRONIC TRANSACTIONS)

- **Mesaj Bütünlüğü;** İşlemler kötü amaçlı bireyler tarafından hesap numarasında veya tutarda değişiklik yapılacak şekilde değiştirilemez.
- **Linkleme;** SET bir tarafa gönderilen eki sadece diğer tarafın okuyabilmesini sağlar. Linkleme ilk tarafın ekin içeriğini okumasına gerek kalmadan ekin doğru olduğunu kontrol edebilmesini sağlar.



4.1.6 KERBEROS



- 80'li yılların sonlarına doğru önerilen ve uygulamaya geçmiş MIT 'de geliştirilmiş güvenli ve kimlik doğrulamalı sunucu erişim sistemidir.
- Aynı zamanda anahtar dağıtım protokolu olan kerberos bu işlemi iki aşamalı olarak gerçekler. Her aşamada bir sonraki aşama için bir bilet temin edilir.
- Bu biletle beraber ikili olarak kullanılacak anahtarlarda taraflar arasında paylaşılır.



KERBEROS



- Kullanıcı ilk olarak kendi şifresini kullanarak Kerberos kimlik doğrulama sunucusundan bilet verme sunucusuna bağlanmak için bir bilet ve anahtar alır.
- Daha sonra bu bilet ve anahtarı bilet verme sunucusunda kullanarak ulaşmak istediği sunucu için bir bilet ve anahtar temin eder. (ilk aşama)
- İlk aşamada sağladığı şifreyi ve bileti kullanarak istediği hizmeti alır.(Bu şifrenin geçerlilik süresi 24 saattir.)




KERBEROS

- Kerberos kullanımı parolaların ağda düz metin olarak iletilmesini önler.
- Kerberos sistemi, kullanıcı adı ve parola bilgilerinizi merkezileştirerek korunmasını ve yönetilmesini de kolaylaştırır.
- Parola bilgilerinizi yerel bir iş istasyonunda veya sunucuda tutma zorunluluğunuzu ortadan kaldırır. Böylece bir makinanın karşılaştacağı tehlikenin diğerlerini etkileme ihtimali azaltılmış olur.



4.2 ULAŞIM (TRANSPORT) GÜVENLİK PROTOKOLLERİ

- Ulaşım Katmanı Protokolü TCP ve UDP ulaşım katmanı protokolleri, bir üst katmandan gelen veriyi paketleyip bir alt katmana verirler.
 - Eğer veri bir seferde gönderilemeyecek kadar uzunsa, alt katmana verilmeden önce parçalara ayrılır (segment) ve her birine bir sıra numarası verilir.
 - Güvenli veri alış iletimini sağlamak amacıyla hata denetim mekanizmaları üzerine kurulmuştur. Katman hata denetiminin yapıldığı son OSI protokol parçasıdır. Eğer fiziksel katman doğru olarak çalışmıyorsa bu katmanın yükleneceği görev yükü daha da artacaktır.
- 

ULAŞIM (TRANSPORT) GÜVENLİK PROTOKOLLERİ



- SSH (Secure Shell/Güvenlik Kabuk)
- SSL (Secure Socket Layer-Güvenli Yuva Katmanı)
- PCT (Private Communication Technology-Kişisel İletişim Teknolojisi)
- TLS (Transport Layer Security-İletim Katmanı Güvenliği)



4.2.1 SSH (SECURE SHELL/GÜVENLİK KABUK)

- SSH ağ üzerinden başka bilgisayarlara erişim sağlamak, uzak bir bilgisayarda komutlar çalıştırmak ve bir bilgisayardan diğerine dosya transferi amaçlı geliştirilmiş bir protokoldür.
- Güvensiz kanallar(internet vs) üzerinden güvenli haberleşme olanağı sağlar. SSH ın sağladığı temel unsurlar;
 - ❖ authentication /Kimlik denetimi
 - ❖ encryption /Şifreleme
 - ❖ Integrity /Bütünlük.



SSH (SECURE SHELL/GÜVENLİK KABUK)

İstemci

Sunucu

Asılama İsteği

Konak Anahtarı + Sunucu Anahtarı

Konak(Sunucu(Oturum Anahtarı))

Oturum(TAMAM)

Açık Konak Anahtarı : 1024 bit RSA

Açık sunucu Anahtarı : 768 bit RSA

Oturum Anahtarı : 256 bit rastgele sayı (Blowfish, DES, 3-DES)

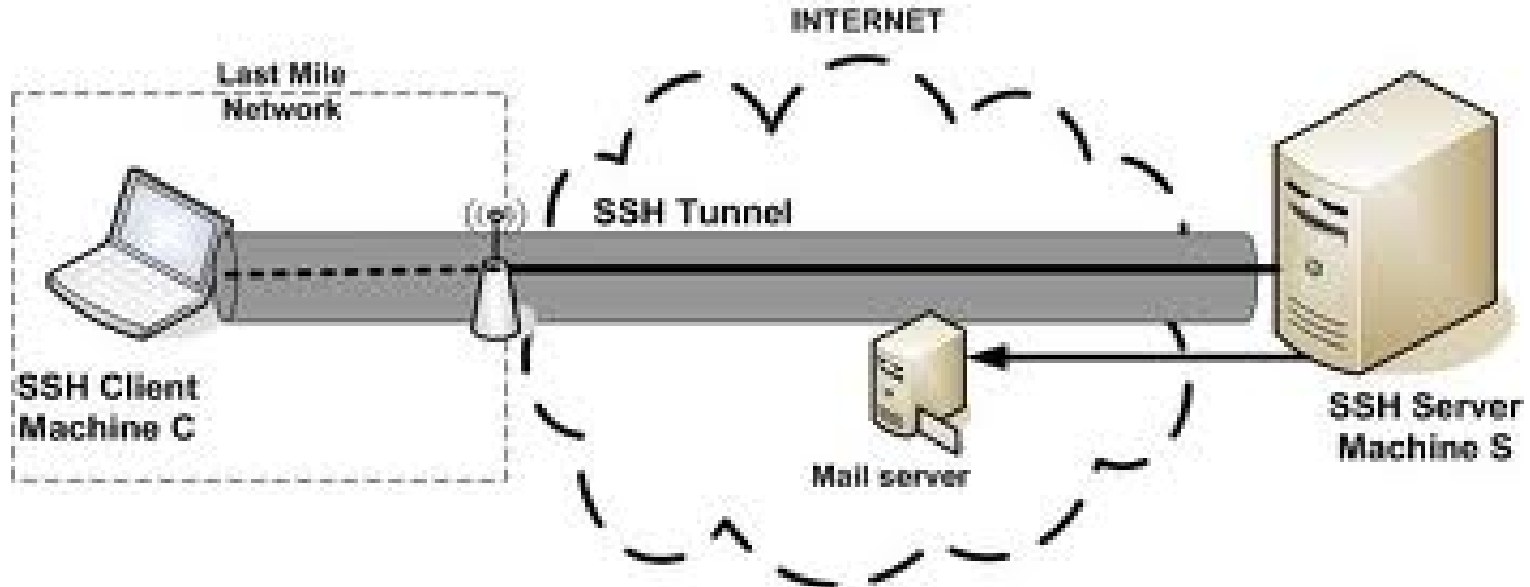
SSH (SECURE SHELL/GÜVENLİK KABUK)

- İstemcinin gönderdiği asıllama isteğine sunucu açık konak anahtarını ve açık sunucu anahtarını göndererek yanıt verir. Konak anahtar çifti konağa özeldir ve sunucunun kurulması sırasında oluşturulur. Bu anahtar daha sonra değiştirilmez. Sunucu anahtar çifti fazladan güvenlik için eklenmiştir.
- Konak aldığı bu anahtarlarla yarattığı bir simetrik oturum anahtarını iki kere şifreleyerek sunucuya gönderir. Ayrıca, yaratılan oturum anahtarına şifrelenmeden önce fazladan güvenlik için rastgele sayılar da eklenir.



SSH (SECURE SHELL/GÜVENLİK KABUK)

- Daha sonra, sunucu oturum anahtarıyla şifrelenmiş bir onay iletisi gönderir. Bu güvenli oturumun ilk iletisidir. Bundan sonraki iletiler oturum anahtarıyla şifrelenmiş olarak iletilecektir.



4.2.2 SSL (SECURE SOCKET LAYER- GÜVENLİ YUVA KATMANI)



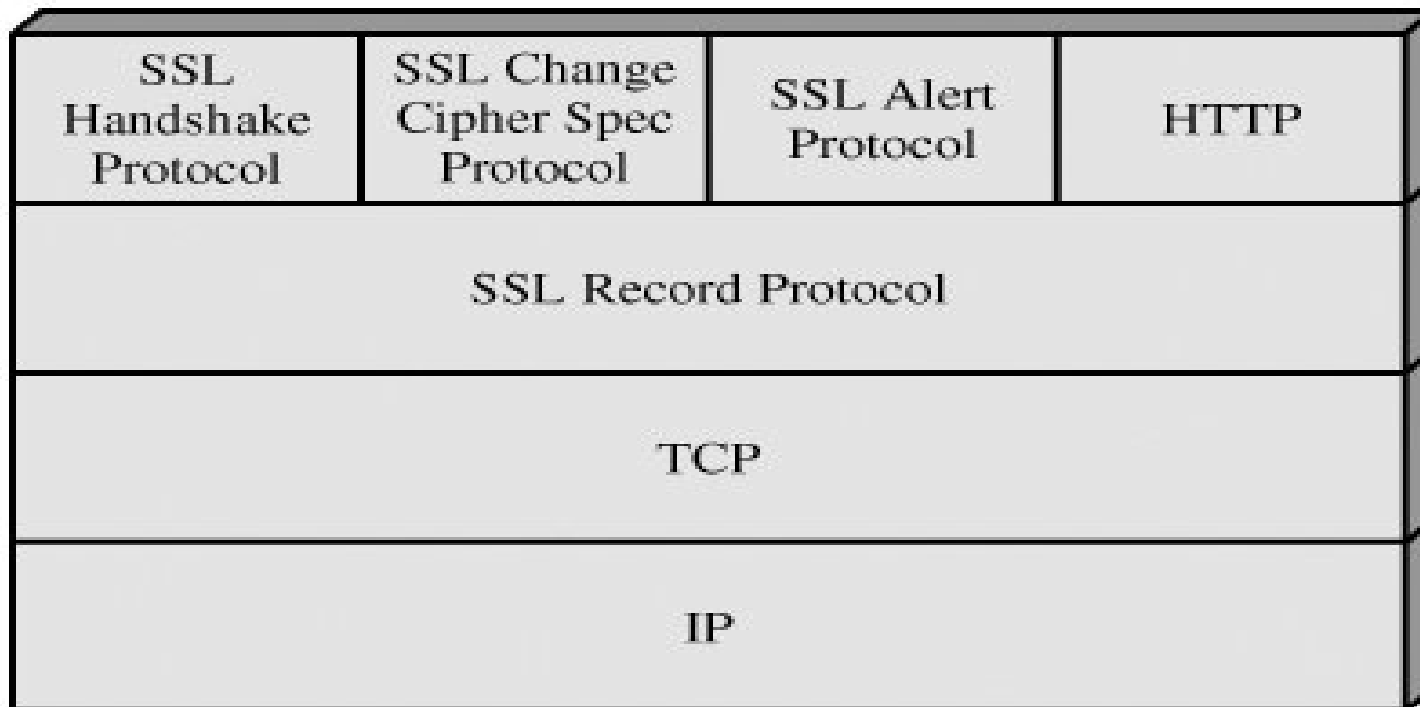
- SSL ilk kez Netscape firması tarafından geliştirilmiş. SSL den sonra yeni standart TLS (Transort Layer Security) olarak adlandırılmaktadır.
- SSL (Secure Socket Layer-Güvenli Yuva Katmanı) verinin iletim ortamından güvenli bir şekilde iletilmesini sağlamak için hem herkese açık anahtar şifrelemesini hemde özel anahtar şifrelemesini aynı anda kullanır.



SSL (SECURE SOCKET LAYER-GÜVENLİ YUVA KATMANI)

○ SSL Mimarisi

- Kayıt Protokolü:Mesaj şifreleme/Doğrulama
- El Sıkışma Protokolü:Kimlik Doğrulama&Anahtar Değişimi
- Uyarı Protokolü:Hata bildirimi
- Şifre Değişim Protokolü: Bekleyen kriptu sırasını etkinleştirmek



SSL (SECURE SOCKET LAYER-GÜVENLİ YUVA KATMANI)

➤ Verinin Değişmediğinden Emin Olunması

- SSL, verinin iletim sırasında değişmediğinden emin olmak için hashing kullanır.
- Sunucu, bir tarayıcıya veri yollayacağı zaman veri den bir hash değeri üretir. Hem veriyi hemde bu hash değerini tarayacıya yollar. Tarayıcı bu bilgileri aldıktan sonra, veriden kendiside aynı algoritmayı kullanarak (hangi algoritmanın kullanılacağı bağlantı kurulurken kararlaştırılır) yenib ir hash değeri üretir ve sunucunun gönderdiği ile aynı değer olup olmadığını kontrol eder. Aynı ise verinin değişmediğindne emin olur. Bu süreç tarayıcının sunucuya veri göndermesi sırasında da işletilir.



SSL (SECURE SOCKET LAYER-GÜVENLİ YUVA KATMANI)



➤ Web Sunucusunun Kimlik Denetimi

- SSL, web sunucusunun kimlik denetimi için sayısal olarak imzalanmış sertifikalar kullanır. Böylece tarayıcı gerçekten alışverişte bulunduğu firma ile bağlantı kurduğundan emin olur.
- Sertifika, bir firma hakkında bilgiler içeren veri yapısıdır. Ayrıca firmanın herkese açık/Özel anahtar çiftinden herkese açık olan anahtarını da içerir. Bu anahtar çifti SSL bağlantı kurma aşamasında (SSL handshake) herkese açık anahtar şifrelemesinde (public key encryption) kullanılır.



SSL (SECURE SOCKET LAYER-GÜVENLİ YUVA KATMANI)



- Sertifikayı isteyen firma, sertifika kendisine geldikten sonra, bu sertifikayı web sunucusuna yükler.
- Sunucuya bir SSL isteği geldiğinde, sertifika tarayıcıya yollanır.
- Tarayıcı sertifikayı aldığı anda sertifikadan firma hakkında bilgileri ve herkese açık anahtarını okuyabilir.
- Tarayıcı gerçekten istediği firmaya bağlantı kurduğunu anlamak için sertifika üzerindeki sayısal imzayı onaylamalıdır.
- Tarayıcı sertifika otoritesinin herkese açık anahtarı ile (bu tarayıcı üzerine kurulum aşamasında yüklenir) sayısal imzayı çözerek otoritenin ürettiği hash değerini elde eder. Daha sonra sertifika içeriğinden kendisi de bir hash değeri üretir ve bu iki değeri karşılaştırır. Eğer aynı ise firma otorite tarafından onaylanmış ve iddia ettiği firmadır.

SSL (SECURE SOCKET LAYER-GÜVENLİ YUVA KATMANI)



➤ SSL El Sıkışması

- SSL el sıkışması tarayıcının ilk kez bir sunucuya SSL isteğinde bulunduğu anda yapılır. EL sıkışma aşamasında aşağıdaki adımlar işletilir.
 1. Tarayıcı ve sunucu iletişim sırasında güvenlik amacıyla kullanılacak olan şifreleme algoritmaları üzerinde anlaşırlar.
 2. Tarayıcı sunucu kimlik denetimi yapar
 3. Tarayıcı simetrik bir anahtar oluşturur ve sunucuya yollar.



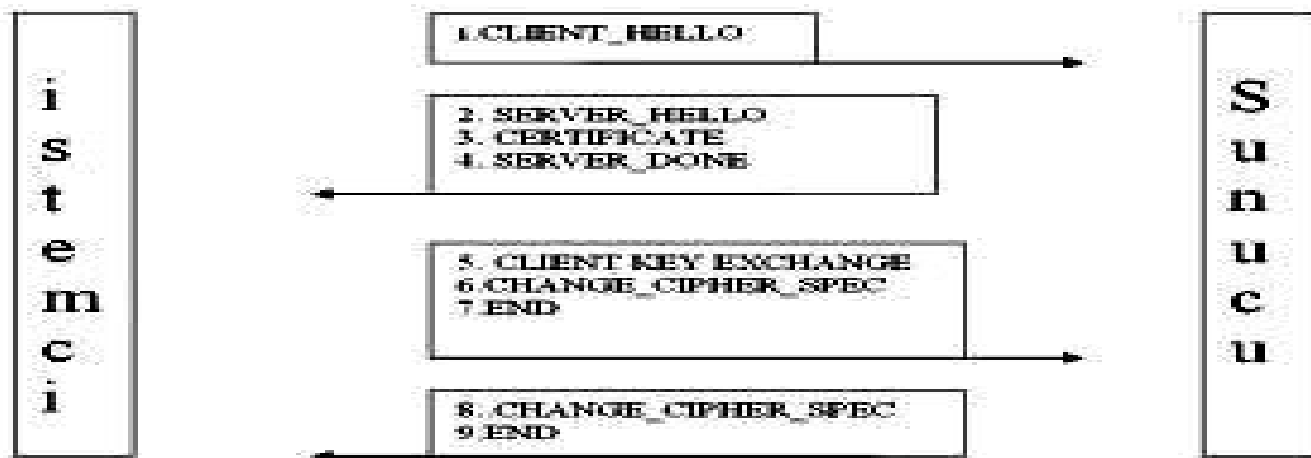
SSL (SECURE SOCKET LAYER-GÜVENLİ YUVA KATMANI)



- El sıkışma protokolü iki safhadan oluşur.
 - Safha 1 , şifreleme algoritma seti üzerinde anlaşma, anahtar değişimi ve sunucunun kimlik denetimi ile ilgilidir.
- Şifreleme seti 3 teknikten oluşmaktadır.
 - ❖ Anahtar değişim tekniği : Sunucu ve tarayıcının el sıkışma sonrasında veriyi şifrelemek için kullanacakları simetrik anahtarı nasıl değiş tokuş yapacaklarını tanımlar.
 - ❖ Simetrik şifreleme tekniği : Bu veri şifrelemesinde kullanılacak olan şifreleme tekniğidir (RC2,RC4..)
 - ❖ Hashing tekniği : Verinin iletim sırasında değişmediğinin testini yapabilmek için sunucu ve tarayıcı tarafından yapılacak hashing tekniğidir.

SSL (SECURE SOCKET LAYER-GÜVENLİ YUVA KATMANI)

- Safha 2 el sıkışması başarılı olursa, ve eğer istenmişse istemcinin kimlik denetimi için kullanılır. El sıkışması sonrasında veri transferi başlar. El sıkışma ve sonrasında gönderilen bütün mesajlar SSL protokol yapısı içinde yollanır.
- Tarayıcının sunucunun kimliğini onaylaması için, sunucu tarayıcıya sertifikasını yollar. Daha önce anlatılan yöntemle tarayıcı sunucunun kimliğini onaylar. Tarayıcı simetrik bir anahtar oluşturur, daha sonra sunucunun herkese açık anahtarı ile bu anahtarı şifreler ve sunucuya yollar. Kendi özel anahtarını kullanarak sunucu şifreli anahtarı çözer. Böylece her iki tarafta iletim sırasında veriyi şifrelemek için kullanacakları ortak bir anahtara sahip olurlar. El sıkışma tamamlanmış olur.



4.2.3 PCT (PRIVATE COMMUNICATION TECHNOLOGY-KİŞİSEL İLETİŞİM TEKNOLOJİSİ)

- PCT (Private communication technology, kişisel iletişim teknolojisi) Microsoft tarafından 1995 yılında Netscape'e karşılık vermek amacıyla çıkarılmış, temelinde SSL 2.0'dan farkı olmayan bir iletişim kuralıdır. Dört ileti ile bağ kurulur. PCT kayıt iletişim kuralı üzerinde çalışan ve PCT tokalaşma iletişim kuralından oluşan iki katlı bir yapısı vardır.



4.2.4 TLS (TRANSPORT LAYER SECURITY-İLETİM KATMANI GÜVENLİĞİ)

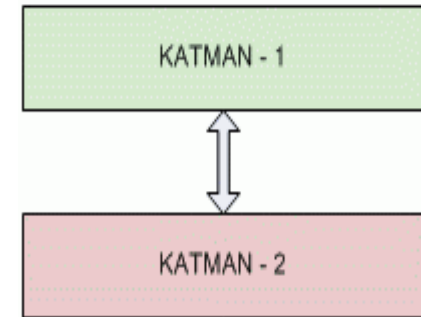


- TLS (İletim Katmanı Güvenliği) internet veya intranetler üzerindeki Web iletişiminin güvenliğini sağlamak için kullanılan standart bir protokoldür.
- Bu protokol, istemcilerin sunucuların kimliğini doğrulamalarını veya isteğe bağlı olarak, sunucuların istemcilerin kimliğini doğrulamalarını sağlar.
- Ayrıca, iletişimi şifreleyerek güvenli bir kanal sağlar.



TLS (TRANSPORT LAYER SECURITY-İLETİM KATMANI GÜVENLİĞİ)

- Protokol iki katmandan oluşur:



- TLS kayıt protokolü; veriler simetrik şifreleme anahtarları ile şifrelenir. Her bağlantı için farklı bir simetrik şifreleme anahtarı kullanılır. Bu anahtar TLS el sıkışma protokolü kullanılarak alıcı ve verici tarafından paylaşılır.
- TLS el sıkışma protokolü; haberleşecek tarafların birbirlerini yetkilendirmeleri, şifreleme algoritması ve anahtarların karşılıklı değişimi sağlanır



TLS (TRANSPORT LAYER SECURITY-İLETİM KATMANI GÜVENLİĞİ)

- TLS, Güvenli Yuvalar Katmanı (SSL) protokolünün en son ve en güvenli sürümüdür.
- Önemli bir farklılık, TLS İleti Kimlik Doğrulaması için Anahtarlı-Karma Kodu (HMAC) algoritması uygularken,SSL İleti Kimlik Doğrulama Kodu (MAC) algoritmasını uygulamasıdır.
- HMAC, MAC ile aynı şekilde bir bütünlük denetim değeri oluşturur.Ancak, bunu, karmanın kırılmasını çok daha zorlaştıran bir karma işlevi yapısıyla oluşturur.

4.2.5 SONUÇLAR



- Anlatılan iletişim kuralları arasında önümüzdeki günlerde varlığını sürdürecekmış gibi görünen, SSL'in devamı olan TLS ve SSH. Küresel anlamda SSL'in bugün dahi yaygın kullanıldığını görüyoruz. SSH ise daha küçük ağlarda da olsa aynı seviyede yaygın kullanılıyor.
- SSL ve TLS'nin uygulama iletişim kurallarının yapılarını değiştirmediklerini ve bu sebeple ancak geçici bir çözüm olarak ele alınması gerektiğini savunanlar da var. Bundan başka bu iletişim kurallarının bağ merkezli olması dolayısıyla karşılaşılan götürüleri var.
- Tamamına bakıldığında, bu katmandaki iletişim kurallarının hiçbirinin trafik çözümlemesine ya da sel (flooding) saldırılarına karşı savunması olmadığı gözden kaçmamalıdır.

KAYNAKLAR

- <http://www.belgeler.com/blg/17hx/ag-guvenligi-ve-guvenlik-duvarinda-vpn-ve-nat-uygulamalari-network-security-and-vpn-and-nat-applications-in-firewall>
- <http://www.slideshare.net/networksguy/computer-network-security-protocols-and-standards>
- <http://ogrenci.hacettepe.edu.tr/~b0244695/baglantilar/protokol.htm>
- <http://tektasi.net/attachments/article/4/pgpsem.pdf>
- <http://ferruh.mavituna.com/pgp-ye-pratik-giris-pgp-kullanimi-ve-e-mail-guvenligi-oku/>
- <http://www.iscturkey.org/2010/2008/2006/pdf/bildiri/60.pdf>
- <http://www.bilgininadresi.net/Madde/48174/Kriptografik-Protokoller>

