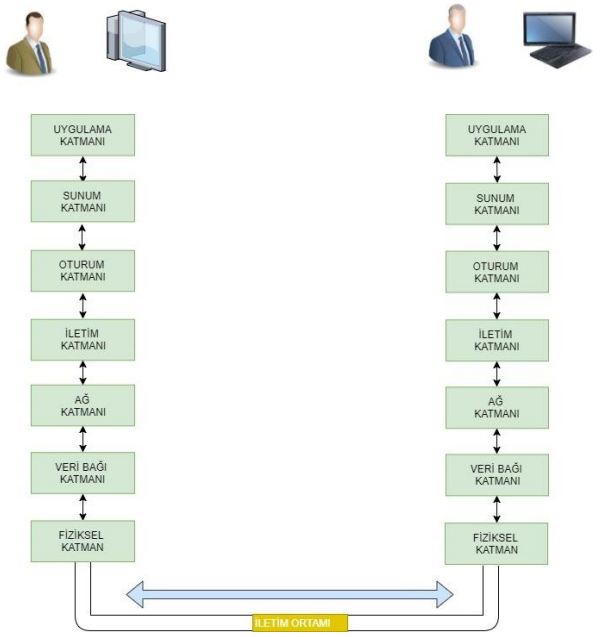
Ebru KARDAŞ 141044049

BİL 470 KRİPTOGRAFİ VE BİLGİSAYAR GÜVENLİĞİ

(08.01.2021)

Araştırma: OSI temel referans modelinin uygulama katmanında (katman 7), ağ katmanında (katman 3) ve taşıma katmanında (katman 4) kriptografik protokollerin uygulanmasının göreli avantajları ve dezavantajlarını araştırarak öneklerle karşılaştırmalı olarak açıklayın.

OSI Modeli



OSI modeli, İngilizce açılımı Open Systems Interconnection olup ağlar oluşturulurken türden ve donanımdan tamamen bağımsız noktalar arasındaki iletişimin nasıl ilerleyeceğine dair bir standart belirlemek için ISO tarafından geliştirilmiştir. Buradaki amaç, ağ mimarilerinin ve protokollerinin bir ağ ürünü bileşeni gibi kullanılmasını sağlamaktır.

7 katmandan oluşan bu modelde her bir katmanın görevi, bir üst katmana servis sağlamaktır. Standartlaşmış bu hiyerarşik model, ağ dizaynı ve yönetiminin daha kolay olmasını sağlar. Her katmanda çalışan protokoller ve bu protokollerin görevleri vardır.

OSI Avantajları:

- Ağ için gerekli donanım ve yazılımların belirlenmesini sağlar.
- Ağ boyunca gerçekleşen işlemlerin iletişimini ve anlaşılmasını sağlar.
- Hata ayıklamada oldukça yararlıdır.

Ebru KARDAŞ 141044049

Katman 3: Ağ Katmanı (Network)

Ağ katmanı, kısaca adresleme yapılan katmandır. Verinin varış noktasına giden en kısa, en uygun yolu bulmak için yönlendirme algoritmalarını kullanarak rota belirler. Bu rota yönlendiriciler tarafından kullanılacaktır. Kaynak ve hedef ağ adresleri (IP) dışında paketin toplam boyutu, TTL, servis tipi, versiyon, hata denetimi gibi bilgiler de bulundurmaktadır. Bu adresleme işlemi dinamik veya statik gerçekleştirilebilir. Mantıksal adreslerin fizikse adrese çevirimi yanı sıra ağ trafiği, yönlendirme, adres planlaması da yapılmaktadır. Uzaktan bağlanma bu katmana bağlıdır.

Güvenlik

Herhangi bir güvencesi ve güvence zorunluluğu yoktur. Açık bir IP adresine denk gelen özel bir adres ile saklama yolu, kapsamlı bir savunma çözümü getirir. Virtual Private Networking (VPN) varlığı, iletişimin şifrelendiği anlamına gelir fakat verinin şifrelendiği anlamına gelmez.

Dynamic Host Configuration Protocol (DHCP) Dinamik Ana Bilgisayar Yapılandırma Protokolü, yönetim kolaylığı, düşük insan hatası riski ve esnekliği olduğu için yaygındır. Ağın yetkisiz erişimden korunmasını sağlar. IP çakışmaları veya uzun oturumlar için DHCP uygun olabilir. DDoS saldırıları, kötü trafik olası risklerdir.

Katman 4: Taşıma/İletim Katmanı (Transport) ***

Taşıma/İletim katmanı, gelen verinin bölütler olarak taşındığı katmandır. Gelen veri, bölüt adı verilen parçalara bölünerek taşınır ve uçtan uca iletim sağlanmış olur. Diğer katmanlarda yapılan hata denetimlerinden sonra hata düzeltme işlemi burada gerçekleştirilir. Gönderici tarafında bölme işlemleri yapılırken, alıcı tarafında başlıktan servis nokta adresi okunarak yönlendirme yapılır ve veri bütünlüğü için sıralama ve toplama işlemleri yapılır. Bağlantıya Dayalı Servis'te alıcı, bir onay göndererek bölüt veya bölüt grubunun gönderildiğinden emin olur (TCP). Bağlantısız Servis ise onay gönderip cevap beklemediği için daha hızlıdır ama daha az güvenilirdir. (UDP)

Güvenlik

Bir bilgisayar sisteminin binlerce bağlantı noktası (port) vardır. Bu bağlantı noktaları 3 farklı kategoride sınıflandırılır: tanınmış (well-known), kaydedilmiş (registered) ve dinamik. Bu noktada güvenlik sağlanır. Örneğin trojanlar belirli TCP ve USP bağlantı noktalarını hedefler. Virüs tarama programları bu korumayı sağlar.

Genişletilmiş Üç Yönlü El Sıkışma, müzakere verilerini ve anahtar değişim verilerini sağlamak için geleneksel TCP el sıkışma tekniklerini genişletir.Durum Geçişi, yetkili aktarımları ayırt etmek için ana bilgisayar durumunu kullanan güvenli bir TCP yöntemidir. Veri bütünlüğü, bir saldırganın verileri değiştirip değiştirmediğini belirlemek için MAC (Mesaj Kimlik Doğrulama Kodu) aracılığıyla sağlanabilir. Veri gizliliği, şifreleme yoluyla elde edilebilir ve veri bütünlüğü ile aynı zamanda ele alınmalıdır.

Ebru KARDAŞ 141044049

Katman 7: Uygulama Katmanı (Application/Desktop)

İnsan-bilgisayar etkileşimini sağlayan, uygulamaların ağ servislerine ulaşabildiği katmandır. Son kullanıcıya en yakın katman olan uygulama katmanı, bilgisayar uygulamaları ile ağ arasında bir köprü görevi görerek ağın kullanılabilmesi için araçlar sunar. İletişim kuracağı bilgisayarın uygun olup olmadığını tespit eder, iletişimi senkronize eder. Diğer katmanlardan farklı olarak sadece bu katman servis **sağlamaz**. E-posta, veritabanı gibi uygulamaların yanında Microsoft API'leri bu katmanda çalışır.

Güvenlik

İletişimde bulunan kişiler, servis kalitesi ve verinin sözdizimi ile ilgili kısıtlamalar tanımlıdır, kullanıcı yetkilendirme ve gizlilik dikkate alınır. En yaygın kimlik doğrulama yöntemi kullanıcı adı ve şifre ikilisidir. Şifrenin uzunluğu, karmaşıklığı, ne sıklıkla değiştirildiği de güvenlik açısından önem arz eder. Windows 2000 ve üstünde kullanılan kimlik doğrulama protokolü Kerberos, zamana duyarlı bir protokoldür.

E-maillerde kullanılan Pretty Good Privacy (PGP) gibi şifreleme yöntemleri bu seviyede gerçeklenir. Çok katmanlı şifreleme kaynak tüketimini arttırsa da veri gizliliğini sağlamanın en iyi yollarındandır.

Bot gibi kötü amaçlı yazılımlara (malware) karşı antivirüs programları kullanılmalıdır.

OSI Modeli				
	Katman	**Veri Birimi**	**İşlevi**	**Protokoller**
3.Ağ	**Ortam**	**Paket/ Datagram**	Çok düğümlü bir ağın, adreslendirme, yönlendirme (routing) ve trafik denetimi gibi süreçler kullanılarak yapılandırılması ve yönetilmesi.	AppleTalk, ICMP, IPsec, IPv4, IPv6, MPLS, ARP, RARP, ICMP, RIP, EIGRP) ISO/IEC 8208, X.25 (PLP), ISO/IEC 8878, X.223, ISO/IEC 8473-1, CLNP X.233, ISO/IEC 10589, IS-IS
4.Taşıma	**Sunucu**	**Bölüt**	Veri bölümlerinin, bölütleme, alındılama ve çoğullama gibi işlemlerle ağ üzerinde noktalara güvenli bir şekilde iletilmesi.	TCP, UDP, DCCP, SCTP
7.Uygulama	**Sunucu**	**Veri**	Kaynak paylaşımı, uzaktan dosya erişimi, dizin hizmetleri veya sanal uçbirimler gibi üst seviye APIler	NFS, SMB, AFP, FTAM, NCP, SMTP, http, FTP, POP3, SNMP SSH, TFTP, DNS

Ebru KARDAŞ 141044049

3. AĞ KATMAN PROTOKOLLERİ				
	Amaç/Görev	Port/Adres Boyu	Tür	Özellikler ve Farklılıklar
IPV4 (İnternet Protokolü Versiyon 4)	Taşıma katmanından gelen hizmet isteklerine cevap vermek	32 bitlik adres	İnternet Katman Protokolü	Açık Tıkanıklık Bildirimi Uçtan uca adreslemede yetersizlik, veri gizliliği ve bütünlüğündeki yetersizlik
IPV6 (İnternet Protokolü Versiyon 6)	Taşıma katmanından gelen hizmet isteklerine cevap vermek	128 bitlik adres	İnternet Katman Protokolü	Daha güvenli iletişim, geliştirilmiş servis kalitesi, otomatik adres yapılandırması, çoklu gönderim desteği. VPN tedarikçileri, IPv6'yı desteklemesi için sunucularını yükseltme konusunda tepkisizler
AppleTalk	Macintosh bilgisayarlar arası iletişim	128 bitlik adres	Protokol Yığını	Belli donanımdaki makinelerin birbirine bağlanmasını sağlaması Farklı marka/donanım makinelere uyumsuzluk.
CLNS/ DECNet (Bağlantısız Ağ Servisi / Connectionless Network Service)	Gelen hizmet isteklerine cevap vermek		Yönlendirme Protokolü	IPv4'e benzerdir. Ana bilgisayarları (uç sistemleri), yönlendiricilerle (ara sistemler) bağlama
ARP (Adres Çözümleme Protokolü / Address Resolution Protocol)	2. katmana ait adres bilinmiyorsa ARP adresi ile fiziksel adres öğrenilir	48 bitlik adres (MAC)	Haberleşme Protokolü	Ağ katmanı adreslerinin veri bağlantısı katmanı adreslerine çözümlenmesini sağlar. İnternet standardıdır. En çok kullanılan ağ arayüzü Ethernet'tir.
ICMP (İnternet Kontrol Mesaj Protokolü/ Internet Control Message Protocol)	Veri alışverişindeki hata ve geri bildirimleri sağlar.		Kontrol Protokolü	Hata mesajları ve TCP/IP yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır.

Ebru KARDAŞ 141044049

4. TAŞIMA KATMAN PROTOKOLLERİ				
	Amaç/Görev	Port/Adres Boyu	Tür	Özellikler ve Farklılıklar
TCP (Gönderim Kontrol Protokolü/ Transmission Control Protocol)	Veri gönderimi	20-60 Bayt (Bölüt/Segment)	Veri İletişim Protokolü	Gelişmiş bilgisayar ağlarında paket anahtarlamalı bilgisayar iletişiminde kayıpsız veri gönderimi sağlar. Gönderim sağlanana kadar deneme yapıldığı için hızlı olmayabilir. UDP'den yavaştır. Bölütler numaralandırılır.
UDP (Kullanıcı Veribloğu İletişim Protokolü/ User Datagram Protocol)	Veri gönderimi	8 Bayt (Veri bloğu/Datagram)	Veri İletişim Protokolü	İletişim kanallarını veya veri yollarını kurmak için önceden haberleşmeye gerek yoktur, bağlantı kurmadan verileri yollar. Fakat mesajın iletilmesi garantilenmediği için güvenilir değildir.
DCCP (Veribloğu Tıkanıklık Kontrol Protokolü/ Datagram Congestion Control Protocol)	Veri gönderimi	12/16 Bayt (Veri bloğu/Datagram)	Veri İletişim Protokolü	Mesaj tabanlı bir taşıma protokolüdür. Çokluortam trafiğini desteklemek için önerilmiştir. Veri iletimi güvenilir değildir. UDP'nin tıkanıklık kontrolü, tokalaşma ve bağlantı kurumu özellikleri eklenmiş veya TCP'nin güvenilirlik, sıralı paket iletimi ve bayt akışı gibi özelliklerinin çıkarılmış hali olarak tanımlanabilir.
SCTP (Akış Kontrol İletişim Protokolü/ Stream Control Transmission Protocol)	Veri gönderimi	12 Bayt + Veri yığını (Veri bloğu/Datagram)	Veri İletişim Protokolü	Mesaj karışıklığı anında mesajların sıralı ve güvenli bir şekilde iletimini sağlar. İşlem yönelimli olduğu yani mesaj parçaları arasında veri transferi gerçekleştirdiği için UDP ile benzerlik gösterirken, TCP akış yönelimli olduğu yani akış olarak taşıdığı için farklıdır.

Ebru KARDAŞ 141044049

7. UYGULAMA KATMANI PROTOKOLLERİ				
	Amaç/Görev	Port	Tür	Özellikler ve Farklılıklar
AFP (Apple Dosya Protokolü/ Apple Filing Protocol)	Ağ üzerinden dosya paylaşımı	548	Şahsi ağ protokolü	AFS (Apple Dosya Servisi/Apple File Service)'nin bir parçası olup Mac İşletim Sistemleri için dosya servisi sunar.
SMTP (Basit Mail Transfer Protokolü/Simple Mail Transfer Protocol)	Basit mail gönderme	25 (şifresiz), 465	Mail Protokolü	Email'i yerel bir istemciden uzaktaki sunucuya ve oradan da alıcının email sunucusuna göndermek için uzak sunucuyla iletişim kurulur.
FTP (Adres Çözümleme Protokolü / Address Resolution Protocol)	Dosya gönderme	21, gönderilirken boş olan		İnternete bağlı iki bilgisayar arasında dosya transferini sağlayan bir protokoldür. Güvenli olarak tasarlanmamıştır.
IMAP (İnternet Mesaj Erişim Protokolü/Internet Message Access Protocol)	Emailleri yerel email istemcilerine almak	143 (şifresiz), 993	Mail Protokolü	Çift yönlüdür. Yalnızca email başlık bilgisi indirilir. Email'in kendisi sunucuda bırakılır.
POP3 (Postane Protokolü 3/Post Office Protocol 3)	Yerel email istemcilerinin uzak email sunucusu ile iletişim kurmasında ve email'leri indirme	110 (şifresiz), 995	Mail Protokolü	Tek yönlüdür. Bu email istemcilerinde genellikle indirilen email'lerin bir kopyasının sunucuda tutulup tutulmaması hakkında bir seçenek olur.
SSH (Güvenli Kabuk/Secure Shell)	İletişimi şifreleyerek ve kimlik doğrulamaları yaparak güvenli bir mekanizma sunma	22 (TCP), (UDP)	Uzak Yönetim Protokolü	Host ile istemci arasında transfer edilen bilgilerin güvenliğinden şifreleme yöntemi ile emin olması

Ebru KARDAŞ 141044049

KRİPTOGRAFİK KATMAN PROTOKOLLERİ				
	Katman	Amaç/Görev	Özellikler ve Farklılıklar	Örnekleri
IPsec (IP Güvenliği)	Ağ	Bulunduğu katman protokolü (IPv6) için güvenlik mimarisi	Veri bütünlüğü ve kaynak asıllama sağlar. Trafik analizine karşı tam güvenliği yoktur. İşletim sisteminden düşük düzeyde destek gerektirir. İstemci ve sunucu tarafında özel yazılım gerektirir.	VPN (Sanal Özel Ağ- Virtual Private Network) RF24XX
SSL (Güvenli Yuva Katmanı- Secure Socket Layer)	Taşıma	Verileri şifreler	Basitliği güçlü yönlerindendir. Sürüm geri alma saldırılarına duyarlı açıklar. Sertifikalar sahte olabilir	IPPS (İnternette Yazıdırma Prokolü)
TLS (Aktarım Katmanı Güvenliği–Transport Layer Security)	Taşıma	Verileri şifreler, güvenli web bağlantıları kurmak için kullanılır.	SSL öncüsüdür. X.509 sertifikalarını destekler. Ortadaki Adam Saldırısına savunmasızdır. Kimlik doğrulama	Tarayıcılarda yaygın olarak kullanılmaktadır.
SSH (Güvenli Kabuk- Secure Shell)	Taşıma	Uzaktan şifreli sunucuları kontrol etmek için kullanılır. (oturum açma, yetkilendirme)	Bağlantının uçlarında dijital sertifika kullanarak doğrular ve şifreler şifrelenerek korunur. Ortadaki Adam Saldırısına savunmasızdır. TCP port 22 üzerinde çalışır. X.509 sertifikalarını destekler.	Putty (SSH istemci) OSSH
PGP (Oldukça İyi Gizlilik(?) - Pretty Good Privacy)	Uygulama	Mail güvenliği	Kişisel kullanım için uygundur. Daha az masraflıdır. Metin şifreleme VPN'de kullanılabilir. Diffie-Hellman Sayısal imza kullanır.	
S/MIME(Güvenli/ Çok Amaçlı İnternet Posta Uzantısı - Secure/Multipurpose Internet Mail Extension)	Uygulama	Mail güvenliği	Endüstriyel kullanım için uygundur. Daha masraflıdır. Metin dışında multimedya dosya şifreleme Yalnızca e-posta hizmetinde kullanılır. Elgamal Sayısal imza kullanır	

HTTPS (Köprü Metin Aktarım Protokolü)	Uygulama	HTTP'nin güvenli uzantısıdır.	TLS/SSL sertifikası yüklenmiş olan web siteleri olan web siteleri sunucu ile güvenli bir bağlantı kurmak için kullanılır. Saldırganların bağlantıya sızarak veri çalınmasını zorlaştırır. Kişisel veri, ödeme gibi verileri korur.	

Kaynaklar:

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/osi-katmanlar%C4%B1

Görsel 1: https://www.beyaz.net/tr/network/makaleler/osi_referans_modeli_ve_katmanli_iletisim_hiyerarsik_ag_modeli.html

https://www.geeksforgeeks.org/layers-of-osi-model/

https://www.imperva.com/learn/application-security/osi-model/

https://en.wikipedia.org/wiki/OSI_model

A Layered Security Model: OSI and Information Security, Kari A. Pace GSEC Practical

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/a%C4%9F-katman%C4%B1-(network-layer)

https://www.tutorialspoint.com/network_security/network_security_layer.htm

https://devrimdanyal.medium.com/k%C4%B1sa-k%C4%B1sa-modern-%C5%9Fifreleme-protokolleri-ve-kar%C5%9F%C4%B1la%C5%9Ft%C4%B1rmas%C4%B1-639db16d1ab8