T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
MÜHENDİSLİK FAKÜLTESİ
BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

OSI BAŞVURU MODELİ KATMANLARINDA KRİPTOGRAFİK PROTOKOLLERİN UYGULANMASI

BİL 470 KRİPTOLOJİ VE BİLGİSAYAR GÜVENLİĞİ DÖNEM PROJESİ RAPORU - BİRİNCİ KISIM

ÖĞRENCİ
Şeyda Nur DEMİR
12 10 44 042

DERS ÖĞRETİM ÜYESİ
Prof. Dr. İbrahim SOĞUKPINAR

DERS ASİSTANI
-

KOCAELİ, 2020

ÖZET

Bu araştırma, OSI temel referans modelinin, uygulama, ağ ve taşıma katmanlarında, kriptografik protokollerin uygulanmasının, göreli avantaj ve dezavantajlarını içermektedir.

GİRİŞ

Temel Bazı Terimler

OSI Nedir?

Open Systems Interconnection (OSI) modeli ISO (International Organization for Standardization) tarafından geliştirimiştir. Bu modelle, ağ farkındalığına sahip cihazlarda çalışan uygulamaların birbirleriyle nasıl iletişim kuracakları tanımlanır.

Referans (Başvuru) Modeli Nedir?

Kişi veya kaynakların, herhangi bir çalışmada referans olarak aldıkları, kaynak olarak başvurdukları ve bunu kaynak gösterdikleri modeldir. İlk OSI standartları 1970'lerin sonlarında ve 1980'lerin başlarında ISO'nun TC 97 (Technical Committee 97), Enformasyon İşletmesi tarafından ortaya çıkartılmıştır. ISO, son OSI standardını 1984'te çıkartmıştır. Bu model kısa sürede kabul görerek yaygınlaşmış ve ağ işlemleri için bir kılavuz olmuştur.

Katman Nedir?

Referans modelleri katmanlara ayrılmıştır. Böylece herhangi bir katmandaki problem, sadece o katmanda çözülür, ve diğer katmanları etkilemez. Herbir katmanın görevi bir üst katmana servis sağlamaktır. İki bilgisayar arasındaki iletişimde katmanlar sırasıyla iletişim kurarlar; eş düzeydeki katmanlar aslında doğrudan iletişim kurmazlar ancak aralarında sanal bir iletişim oluşur.

OSI Referans Modeli Katmanları Nelerdir?

OSI referans modeli yedi katmandan oluşmuştur. Her katmanda, aktarılan veri farklı bir isim alır. Alt katmanlarda bit katarı, çerçeve, paket gibi isimler verilirken, üst katmanlara gidildikçe isimlendirme ulaşım katmanı protokolü veri birimi (Transport Protocol Data Unit - TPDU) gibi katmana özel hale gelir. Bu katmanlar sırasıyla uygulama katmanı, sunum katmanı, oturum katmanı, taşıma katmanı ağ katmanı, veri iletim katmanı ve fiziksel katmandır.

Kriptografi Nedir?

Kriptografi ya da 'şifreleme' okunabilir durumdaki bir verinin içerdiği bilginin istenmeyen taraflarca anlaşılamayacak bir hale dönüştürülmesinde kullanılan yöntemlerin tümüdür. Kriptografi bir matematiksel yöntemler bütünüdür ve önemli bilgilerin güvenliği için gerekli gizlilik, aslıyla aynilik, kimlik denetimi, ve asılsız reddi önleme gibi şartları sağlamak amaçlıdır. Bu yöntemler, bir bilginin iletimi esnasında ve saklanma süresinde karşılaşılabilecek aktif saldırı ya da pasif algılamalardan bilgiyi -dolayısıyla bilginin göndericisi, alıcısı, taşıyıcısı, konu edindiği kişiler ve başka her türlü taraf olabilecek kişilerin çıkarlarını da- koruma amacı güderler.

Protokol Nedir?

Bir işleyişin düzgün çalışması ve hata yapılmaması için oluşturulan kurallar silsilesine protokol denir. İletişim protokolü veya ağ protokolü, iki ya da daha fazla bilgisayar arasındaki iletişimi sağlamak amacıyla verileri düzenlemeye yarayan, standart olarak kabul edilmiş kurallar dizisidir.

Kriptografik Protokoller Nedir?

Güvenlik (kriptografik protokol), güvenlik ile ilgili bir işlemi uygulayan, bir dizi kriptografik algoritmaları kullanan soyut bir protokoldür. Böyle bir protokol, bu algoritmaların nasıl kullanacağını tanımlar. İzleyenlerin bir veya daha fazlasını kriptografik protokol içerebilir

Kriptografik Protokol Uygulamaları Nelerdir?

Gizli anahtar paylaşımı, varlığının kimlik denetimi, simetrik şifreleme, inkar edilememezlik metodları kriptografik protokollerin uygulama alanlarına örnek olarak verilebilir.

İSTENENLER

OSI Referans Modeli Katmanlarında Uygulanan Kriptografik Protokoller Nelerdir?

OSI Referans modelinin uygulama katmanı için HTTP, FTP, SMTP, sunum katmanı için ASCII, JPEG, PGP, oturum katmanı için NetBIOS, DHCP, taşıma katmanı için TCP, UDP, SPX, ağ katmanı için IP, IPX, veri iletim katmanı için Ethernet, Frame Relay, ISDN ve fiziksel katman için Bit, Kablo, Konnektör, kullanılan protokollere örnek olarak verilebilir.

Şifrelemenin Konumlandırılması

Veri iletimi aşamalarında, ağ üzerinde şifreleme, iki şekilde konumlandırılabilir, ilki bağlantı şifreleme, ikincisi uçtan uca şifrelemedir.

Bağlantı Şifreleme

Bağlantı şifreleme, ağ üzerinde veri iletilirken, her bağlantıda diğerlerinden bağımsız bir şekilde şifreleme gerçekleştirilir. Her bağlantı, şifreleme cihazı ve bir çift anahtar gerektirir. Burada, veri tamamen şifrelenir, ve başlık bilgisi her bağlantıda, yeni bağlantı bilgileri ile değiştirilir. Bunun avantajı, verinin iletilirken olası saldırılarda, haberleşen kaynaklar arasında bilgi vermemesi, trafik analizine engel olmasıdır. Ancak dezavantajı, daha çok şifreleme cihazı gerektirmesi, her bağlantıda ayrı anahtarın kullanılması, daha maliyetli olması ve her bağlantıda şifreleme yapıldığı için daha yavaş çalışmasıdır.

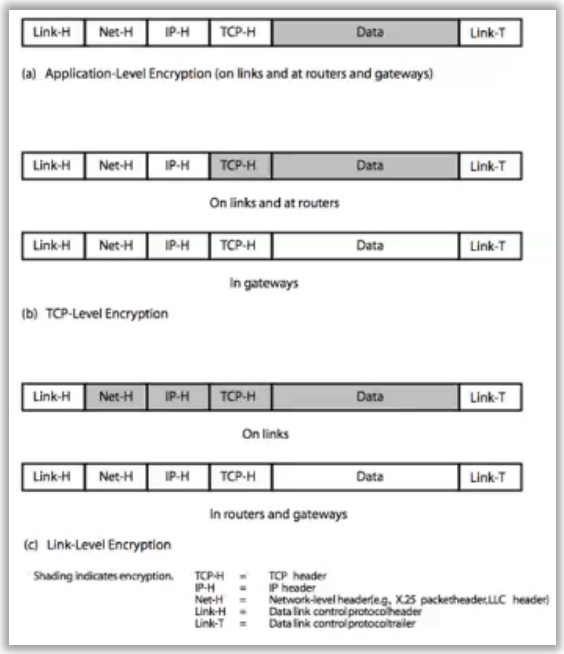
Uçtan Uca Şifreleme

Uçtan uca şifreleme, şifreleme orijinal kaynak ile varış arasında gerçekleştirilir, gerekli olan şifreleme cihazları, her iki uçta birer cihaz ve paylaşılmış anahtarların olması gerekir. Burada, veri içeriği şifrelenir, kimlik doğrulaması sağlanır, paketin başlığı şifrelenmez. Bunun avantajı, sadece başta ve sonda şifreleme gerçekleştiği için daha az maliyetli olması ve daha hızlı olmasıdır. Ancak dezavantajı, paketin başlık bilgisi açık taşındığı için, haberleşen kaynaklar hakkında bilgi vermesi, ve ağda daha fazla güvenlik ihlaline sebep olması, trafik analizine engel olamamasıdır.

OSI Referans Modelinde Şifrelemenin Katmanlarda Konumlandırılması

OSI'de fiziksel katmanda ve veri iletim katmanında bağlantı şifreleme uygulanırken, ağ katmanı, taşıma katmanı, sunum katmanı ve uygulama katmanında uçtan uca şifreleme uygulanır. Daha üst katmanlara çıktıkça, daha az veri şifrelenir, ve daha fazla anahtar kullanılması gereklidir.

OSI Referans Modelinde Şifreleme ve Protokol Seviyeleri Arasındaki Bağlantı



OSI Başvuru Modelinde Bazı Katmanlarda Kriptolojik Protokollerin Uygulanmasının Kıyaslanması

KATMAN 7	**KATMAN 4**	**KATMAN 3**
UYGULAMA KATMANI	**TAŞIMA KATMANI**	**AĞ KATMANI**
Görevi	**Görevi**	**Görevi**
Kullanıcının uygulamaları	Verinin bölümlere ayrılarak karşı tarafa gitmesinin kontrol edilmesi	Veri bölümlerinin paketlere ayrılması, ağ adreslerinin fiziksel adreslere çevrimi
		Teknik olarak daha üstündür
	İşletim sistemini değiştirmez, sadece uygulama ile ilgilenir	Uygulamayı değiştirmez, sadece işletim sistemi ile ilgilenir
		API değişmediği sürece kimlik doğrulamadan geçemez
	Deploy etmesi, canlıya geçirmesi daha kolaydır	Outboard Hardware Process daha kolaydır
Şifreleme Konumlandırılması	**Şifreleme Konumlandırılması**	**Şifreleme Konumlandırılması**
Uçtan uca şifreleme	Uçtan uca şifreleme	Uçtan uca şifreleme
Cihaz	**Cihaz**	**Cihaz**
Gateway (Ağ geçidi)	Gateway (Ağ geçidi)	Router (Yönlendirici) Switch (Köprü)
Kullanılan Veri	**Kullanılan Veri**	**Kullanılan Veri**
Data bits (Veri bitleri)	Segment (Bölüm)	Packet (Paket)
Kullanılan Protokoller	**Kullanılan Protokoller**	**Kullanılan Protokoller**
HTTP, FTP, SMTP	TCP, UDP, SPX	IP, IPX
Anahtar Değişimi	**Anahtar Değişimi**	**Anahtar Değişimi**
	SSL/TLS	IPSec

KAYNAKLAR

1. OSI Modeli Hakkında, https://tr.wikipedia.org/wiki/OSI_modeli
2. Kriptografi Hakkında, https://tr.wikipedia.org/wiki/Kriptografi
3. İletişim Protokolleri Hakkında, https://tr.wikipedia.org/wiki/%C4%B0leti%C5%9Fim_protokol%C3%BC
4. Katmanlı İletişim Hakkında, https://www.beyaz.net/tr/network/makaleler/osi_referans_modeli_ve_katmanli_iletisim_hiyerarsik_ag_modeli.html
5. OSI Katmanları Hakkında, https://www.beyaz.net/tr/ipucu/entry/14/katman-katman-katmerli-osi-layer

RAPOR SONU

SON DEĞİŞİKLİK : 08.01.2021 17:15

ÖĞRENCİ
Şeyda Nur DEMİR
12 10 44 042

DERS ÖĞRETİM ÜYESİ
Prof. Dr. İbrahim SOĞUKPINAR

DERS ASİSTANI
-

KOCAELİ, 2020