BIL 470 – KRİPTOGRAFİ VE BİLGİSAYAR GÜVENLİĞİ

MEDİNE ASLAN

161044015

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 Nedir?

OSI'de amaç iki bilgisayar arası iletişimin nasıl olacağını tanımlamaktır. 7 katmanı vardır ve bu katmanlardaki protokolleri uygulamak amacıyla bir bilgisayar ağ çerçevesi tanımlar. Ağ oluşturmada protokoller bir tür müzakere ve iki ağ kuruluşu arasındaki kuraldır. Şu katmanlardan oluşur:

Katman 7: Uygulama Katmanı

Bu katman kullanıcıya en yakın olan katmandır. Programın network için ihtiyaç duyduğu fonksiyonları kapsar. Aralarından sadece bu katman diğer katmanlara hizmet sağlamaz.

SSH, telnet, FTP, TFTP, SMTP, SNMP, HTTP, DNS, HTTPS protokolleri ve tarayıcılar bu katmanda çalışır.

Katman 6: Sunum Katmanı

Bu katman gönderilen verinin alıcı tarafından anlaşılacak bir forma dönüşütürülmesini sağlar. Dosya uzantıları bu katmanda belirlenir. Verinin şifreleme ve deşifrelemesi de bu katmanda uygulanır.

Katman 5: Oturum Katmanı

İletişim kuran cihazlar arasındaki oturumlar olarak bilinen diyalogları kontrol eder. Oturum açılmasını, yönetilmesini ve kapatılmasını kapsar.

Katman 4: Taşıma Katmanı

İlerlemesi yapılacak olan verinin bir zarara uğramadan hedefe ulaşmasını sağlar. Datayı bölümlere ayırır ve alıcı tarafında tekrar birleştirir. Datanın hedefe ulaşıp ulaşmadığını da kontrol eder. Eğer data hedefe ulaşmamışsa tekrar gönderilmesini sağlar. TCP, UDP, SPX, RTP, SIP, H.323 katman 4'te kullanılan protokollerdendir.

Katman 3: Ağ Katmanı

Bu katman veri paketinin farklı bir ağa gönderilmesi gerektiğinde hedef adres bilgilerinin eklendiği katmandır. Adresleme işlemi iki farklı şekilde yapılır. Bunlar DHCP protokolü ile

veya manuel olarak gerçekleştirilir. IP, IPX, IPSec, AppleTalk DDP, ARP, RARP, ICMP, RIP, EIGRP katman 3'te kullanılan protokollerdendir.

Katman 2: Veri Bağlantı Katmanı

Bu katman fiziksel katmana erişmek için gerekli kuralları belirler. Bu katmanda Ethernet ya da Token Ring olarak bilinen erişim yöntemleri çalışır ve bu erişim yöntemleri verileri kendi protokollerine uygun olarak işleyerek iletirler. Bu katmanda veriler parçalara bölünür ve bu parçalara frame denir. Switch ve bridge bu katmanda çalışır.

Katman 1: Fiziksel Katman

Datanın iletilirken kablo üzerinde dönüşeceği fiziksel yapıyı belirler. Hub ve repeater bu katmanda çalışır.

Katman 7 , 4 ve 3' te Uygulanan Kriptografik Protokoller

Katman 7 (Uygulama Katmanı): SSH, HTTPS

Katman 4 (Taşıma Katmanı): TCP

Katman 3 (Ağ Katmanı) : IPSec

HTTPS Protokolü

OSI'nin 7. Katmanında bulunan kriptografik protokoldür. Erişilen web sitesinin kimlik doğrulaması ve aktarılan verilerin alışverişi sırasında gizliliğin ve bütünlüğün korunmasını amaçlar. Saldırılara karşı koruma sağlar.

Avantajları

En önemli avantajlarından birisi veri şifrelemedir.

http veri aktarımı yaparken verileri şifrelemez. Herhangi biri araya girerse, veriler kötü kişilerin eline geçer. HTTPS üzerinden aktarılan veriler şifrelenir bu yüzden daha güvenlidir.

El sıkışması yolu ile veri doğrulama işlemini yapar.

Verilerin doğru yerlere gönderileceğini garanti eder.

Verileri kaydetmediği için veri korumasını sağlar.

Dezavantajları

Kullanımı için SSL sertifikası gerekmektedir.

Hesaplama sayısı çok fazla olduğu için yanıt süresi gecikir. Web hızı diğer protokollere göre düşüktür.

TCP Protokolü

Kayıpsız veri gönderimini sağlamak amaçlı geliştirilmiştir. 4. katman protokollerinden birisidir. Popüler veri iletimleri TCP vasıtası ile yapılır. Verilerin hedefe ulaşmasını, zamanında ulaşmasını ve kopyalanmamasını garanti eder.

Avantajları

Protokol paketleri kolayca değiştirilebilir.

Tüm işletim sistemleri ile uyumlu olduğundan diğer sistemler ile kolayca iletişim kurabilir.

Her türlü donanım ve bilgisayar ağları ile uyumludur.

Ağ üzerinden en verimli yolu belirleyebilir.

Dezavantajları

Verinin karşı tarafa ulaşıp ulaşmadığını kontrol ettiği için yavaştır.

Verilen her zaman istenilen zamanda gönderilmeyebilir.

Çok noktaya gönderim sağlayamaz.

Paketlerin tekrardan iletilmesi ek yük oluşturur. Bu tarz durumlarda TCP yerine UDP kullanmak mantıklıdır. Buna örnek olarak HD videoları gösterebiliriz. TCP kullanılıyorsa, yeniden iletimden dolayı bant genişliğinden fazlasına ihtiyaç duyulur. Böyle bir durumda TCP yerine UDP kullanmak mantıklıdır.

IPSec Protokolü

IP ağ trafiği için oluşturulmuş bir güvenlik hizmeti altyapısı tanımlar. IPSec'in temel kullanım amacı, ağ verisini korumaktır. Tünelleme kullanarak iki uç nokta arasında iletilen verinin şifrelendiği bağlantılar kurarak gerçekleştirilir. OSI'nin 3. Katmanında bulunur.

Avantajları

TCP Protokolü oluşturulurken güvenlik üzerinde pek fazla durulmamıştır fakat IPSec protokolü sayesinde veriler ağ üzerinde güvenli bir şekilde hedefe ulaştırılır.

Bağlantı kopma durumunda güvenli şekilde bağlantı sağlar.

Uygulama ayarları değişmiş olsa bile bağlantı devam eder.

Dezavantajları

Karmaşıklık vardır ve zaman zaman anlaşmazlıklar meydana gelir.

Geniş erişim aralığına sahiptir. Tek bir cihaza erişim verilmesi, diğer cihazlar için de erişim ayrıcalıkları sağlayabilir.

Uyumluluk sorunları ile karşılaşılır.

Bazı Karşılaştırmalar

Katman 4'te TCP katman 3'te ise ip adreslerinin protokolleri kullanılır. Bu yüzden bu katmanlarda şifreleme yaptığımız zaman uçtan uca gerçek zaman haberleşmesi engellenmiş oluyor.

Katman 4'te işletim sistemi değişmiyor sadece uygulamalar değişiyor.

Katman 4'teki şifreleme protokol veya hangi protokol kullanılıyorsa onlar şifreleniyor.

Katman 4'ü deploy etmek daha kolaydır.

Katman3'te uygulamalar değiştirilmiyor. Uygulamalardaki API'lar değiştirilmiyor. Sadece işletim sistemi değişiyor.

Katman3 öncelikli olarak ip protokolleri ile ilgilenir. API değişiklileri olmadıkça 3. Katman kimlik doğrulamasına geçemez. Dolayısıyla katman 3'teki şifreleme genellikle bağlantılar arası şifreleme şeklinde gerçekleşiyor.

Programlama Projesi

a) Projenin bu partında bizden AES simetrik şifreleme algoritması gerçekleyerek şifreleme ve deşifrelemede kullanılması istenmiştir. (Test verileri ile birlikte)

   Projemi 128 bytelık olarak gerçekledim. Ve python 2.7.18 kullanarak çalıştırdım. Bu partı gerçeklerken öncelikle tur anahtarlarının bulunmasını sağladım. Tur anahtarlarını bulmak için substitionBytes, shiftRow, mixColumns, addRound, galois_mult fonksiyonlarını kullandım. Bu fonksiyonlar sayesinde AES tur anahtarlarını bulup AES şifreleme algoritmasını gerçekledim.

   Bu işlemleri yapmamın sebepleri ve nasıl bir sıralamada gerçeklediğim ise şu şekildedir:

   Öncelikli olarak verilen anahtarın oluşturulmasını sağladım. Bunun için keyExpand fonksiyonunu kullandım. Burada amaç esas anahtarın kullanılarak algoritmanın turlarında kullanılacak tur anahtarlarının oluşturulmasıdır.

   İlk çevrim için addRound fonksiyonunu kullandım. Bu fonksiyon bulunan state'in ilk tur anahtarı ile XOR'lanmasını sağlamaktadır. Tur anahtarı baytlara bölündükten sonra sıra ile matrisin elemanları ile XOR'lanır.

   Diğer turların bulunması için ise sırasıyla şu işlemleri uyguladım:

   1) **Byteların değiştirilmesi işlemi(Substition Bytes):** State matrisindeki her byte'ın S Box tablosuna göre güncellenmesidir. Bu güncelleme doğrusal olmayan bir dönüşüm ile yapılır. Bu işlem için substitionBytes fonksiyonunu kullandım.

2) **Satır Kaydırma İşlemi(Shift Rows):** Burada her satırın gereken miktarda kaydırılmasını gerçekledim. AES'de ilk satır sabit kalırken 2. 3. ve 4. satırlar sırası ile 1, 2 ve 3 byte sola kaydırılır. Bunun için shiftRows fonksiyonunu kullandım.

3) **Sütun Karıştırma İşlemi(Mix Columns):** Burada her sütundaki 4 byte'ı birbirleri ile karıştımayı amaçladım ve bunu mixColumns fonksiyonunu kullanarak gerçekledim. Sütun karıştırma (mixColumns) fonksiyonu 4 bayt girdi alıp 4 bayt çıktı verir ve girdideki her baytın çıktıdaki her bayt değerini etkilemesini sağlar.

4) **Son tur** bulunmasını ise sırasıyla şu fonksiyonları kullanarak gerçekledim:

substitionBytes (byte değiştirme işlemi)
shiftRows(satır kaydırma işlemi)
addRound(anahtar ekleme işlemi)

Bu işlemleri AES simetrik şifreleme algoritmasını kullanarak şifreleme yapmak için kullandım. Deşifreleme yapmak için yazdığım bu fonksiyonlardan gerekenlerinin ters şekilde çalışanlarını kullandım. Burada sırasıyla şöyle bir akış uygulanır:

Ters Byte Değiştirme: Ters bayt değiştirme işlemi için bayt değiştirme işleminde olduğu gibi bir tablodan faydalanılır. Şifrelemenin aksine burada ters çevrilmiş S box kullanılır. Bu tablodaki veriler S Box tablosundaki verilerin tersleridir.

Ters Satır Kaydırma: Satır kaydırma adımında yapılan işlemleri sağa kaydırarak gerçekledim.

Ters Sütun Karıştırma: Ters sütun karıştırma adımında ise yine sütun karıştırma adımına benzer işlemler yapılır ancak bu kez farklı bir matris kullanılır.

Tur Anahtarıyla Toplama: Tur Anahtarıyla Toplama adımı genişletilmiş anahtarın içerisindeki son anahtardan başlayarak geriye doğru ilerler. Yani şifreleme için kullandığımız son anahtar deşifreleme için kullandığımız ilk anahtar olur.

Böylelikle bu işlemleri kullanarak AES simetrik şifreleme algoritması ile şifreleme ile deşifreleme gerçekledim. Daha sonra bu şifreleme ve deşifreleme algoritmasını iki farklı test verisi ile test ettim. Bu test metinlerinden birincisi 'Bu test metnidir' ikincisi ise 'Merhabalar Dünya' dır. Test sonuçları şu şekildedir:

```
C:\Users\medo\Desktop>py -2 Aes.py

============================AES Test1================================

Acik Metin: Bu test metnidir
Anahtar: [181, 144, 56, 201, 107, 233, 211, 157, 179, 206, 87, 216, 185, 82, 145, 58]
Sifrelenmis Metin: [239, 209, 48, 24, 148, 254, 189, 142, 58, 77, 4, 207, 246, 200, 205, 180]
Desifrelenmis Metin: Bu test metnidir

============================AES Test2================================

Acik Metin: Merhabalar Dunya
Anahtar: [181, 144, 56, 201, 107, 233, 211, 157, 179, 206, 87, 216, 185, 82, 145, 58]
Sifrelenmis Metin: [53, 146, 183, 11, 58, 231, 198, 243, 231, 56, 54, 131, 246, 240, 210, 50]
Desifrelenmis Metin: Merhabalar Dunya
```

b) Gerçeklenen Şimetrik şifreleme algoritması kullanılarak CBC ve OFB modlarında çalışmayı gerçeklemek ve testlerini yapacak şekle getirmek.

Bu partı gerçeklerken a partında gerçekleğiğim AES simetrik şifreleme ve deşifreleme algoritmalarını kullandım. Bunun için Aes algoritmasını gerçeklediğim dosyada istenen modları gerçeklemek için bir class oluşturdum(class AESModeOfOperation).

Bu class içerisinde encrypt ve decrypt fonksiyonlarında AES algoritması için gerçeklediğim encrypt ve decrypt fonksiyonlarını kullandım. Ve bu fonksiyonların içerisinde CBC ve OFB modları için ayrı ayrı işlemler gerçekledim. Bu işlemler şu şekilde gerçeklenmiştir:

CBC Modu

CBC modunda her açık metin bloğu şifrelenmeden önce bir önceki kapalı metin bloğu ile XOR işlemine sokulur. Böylece her kapalı metin bloğu kendisinden önce gelen tüm açık metinlere bağımlı olmuş olur. Bir mesajın aynı anahtar altında tekrar şifrelendiğinin anlaşılamaması için ilk blokta ilklendirme vektörü(IV) kullanılır.

CBC Modunun matematiksel şifreleme ifadesi şu şekildedir.

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

CBC Modunun matematiksel deşifreleme ifadesi ise şu şekildedir.

$$P_i = D_K(C_i) \oplus C_{i\ 1}, C_0 = IV.$$

Bu modu test etmek için ‘Merhabalar Dünya’ açık metnini kullandım. Test sonucum şu şekildedir:

OFB Modu

OFB modu bir blok şifresini bir senkron akış şifresi haline getirir. Anahtar akışı blokları oluşturur ve bunlar daha sonra şifreli metin üretmek için şifresiz metin bloklarıyla XOR'lanır. Diğer akış şifrelerinde olduğu gibi, şifreli metinde bir bit döndürmek şifresiz metinde aynı konumda döndürülmüş bit üretir.

XOR operasyonunun simetri özelliğinden dolayı şifreleme ve deşifreleme aynıdır ve şu şekildedir:

$$C_j = P_j \oplus O_j,$$
$$P_j = C_j \oplus O_j,$$
$$O_j = E_K(I_j),$$
$$I_j = O_{j-1},$$
$$I_0 = \mathrm{IV}.$$

Bu modu test etmek için 'Merhabalar Dünya' açık metnini kullandım. Test sonucum şu şekildedir:

```
=========================OFB Mode Testi==============================

Acik Metin: Merhabalar Dunya
Anahtar:  [189, 244, 39, 255, 28, 247, 208, 211, 102, 215, 108, 81, 135, 127, 150, 178]
Sifrelenmis Metin: [94, 197, 70, 56, 28, 1, 35, 171, 75, 220, 46, 143, 0, 243, 183, 192, 86, 20, 102, 207, 141, 197, 18, 110, 5, 241, 104, 51, 127, 229, 30, 143]
Desifrelenmis Metin: Merhabalar Dunya
```

AES şifreleme ve deşifrelemeyi, CBC mod ve OFB modu gerçeklediğim programımın genel test çıktısı ise şu şekildedir:

```
Administrator: C:\WINDOWS\system32\CMD.exe
Microsoft Windows [Version 10.0.19041.685]
(c) 2020 Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\medo>cd Desktop

C:\Users\medo\Desktop>py -2 Aes.py

============================AES Test1=============================

Acik Metin: Bu test metnidir
Anahtar: [181, 144, 56, 201, 107, 233, 211, 157, 179, 206, 87, 216, 185, 82, 145, 58]
Sifrelenmis Metin: [239, 209, 48, 24, 148, 254, 189, 142, 58, 77, 4, 207, 246, 200, 205, 180]
Desifrelenmis Metin: Bu test metnidir

============================AES Test2=============================

Acik Metin: Merhabalar Dunya
Anahtar: [181, 144, 56, 201, 107, 233, 211, 157, 179, 206, 87, 216, 185, 82, 145, 58]
Sifrelenmis Metin: [53, 146, 183, 11, 58, 231, 198, 243, 231, 56, 54, 131, 246, 240, 210, 50]
Desifrelenmis Metin: Merhabalar Dunya

=========================CBC Mode Testi=============================

Acik Metin: Merhabalar Dunya
Anahtar:  [224, 46, 61, 195, 205, 19, 181, 236, 245, 161, 81, 38, 249, 181, 2, 177]
Sifrelenmis Metin: [14, 146, 209, 126, 123, 128, 81, 160, 78, 83, 11, 113, 54, 132, 247, 210, 255, 16, 122, 4, 175, 21, 121, 227, 105, 241, 154, 10, 253, 246, 6, 206, 248, 92, 10, 145, 193, 212, 157, 141, 2, 151
, 58, 181, 145, 89, 27, 248]
Desifrelenmis Metin: Merhabalar Dunya

=========================OFB Mode Testi=============================

Acik Metin: Merhabalar Dunya
Anahtar:  [189, 244, 39, 255, 28, 247, 208, 211, 102, 215, 108, 81, 135, 127, 150, 178]
Sifrelenmis Metin: [94, 197, 70, 56, 28, 1, 35, 171, 75, 220, 46, 143, 0, 243, 183, 192, 86, 20, 102, 207, 141, 197, 18, 110, 5, 241, 104, 51, 127, 229, 30, 143]
Desifrelenmis Metin: Merhabalar Dunya

C:\Users\medo\Desktop>
```

Referanslar

https://medium.com/@yavuzunver/aes-ile-veri-%C5%9Fifreleme-daef840f10f3#:~:text=AES%20simetrik%20bir%20%C5%9Fifreleme%20algoritmas%C4%B1d%C4%B1r,192%20veya%20256%20bit%20olabilir.

https://tr.wikipedia.org/wiki/AES#:~:text=AES%20(Advanced%20Encryption%20Standard%3B%20Geli%C5%9Fmi%C5%9F,(kripto)%20standard%C4%B1%20olarak%20kullan%C4%B1lmaktad%C4%B1r.

https://tr.wikipedia.org/wiki/Blok_%C5%9Fifre_%C3%A7al%C4%B1%C5%9Fma_kipleri

https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/ipsec-vpn-(internet-protocol-security-internet-protokol%C3%BC-g%C3%BCvenli%C4%9Fi)

https://fabian-voith.de/2020/07/29/which-layer-for-encryption-which-for-vpns/#IPsec_vs_TLS

https://medium.com/bili%C5%9Fim-hareketi/osi-modeli-ve-7-katman-7c3bb467798c