

IPSEC  
IKE  
ŞİFRELEME STANDARTLARI

Devrim Kalmaz

20.07.2006

[dkalmaz@hotmail.com](mailto:dkalmaz@hotmail.com)  
[devrimkalmaz@yahoo.com](mailto:devrimkalmaz@yahoo.com)

## Sayfa.3

- IPSEC Nedir?
- Esp Encapsulation Security Payload
- Ah Authentication Header

## Sayfa.4

- IKE
- Phase 1

## Sayfa.5

- Phase 2

## Sayfa.6

- Feistel Cipher Çizim

## Sayfa.7-8

- IKE Phase 1

## Sayfa.9

- IKE Phase 2

## Sayfa.10

- ESP / AH

## Sayfa.11

- Diffie-Hellman Çizimler

Günümüzde sıkça bahsi geçen bu kavramlar hakkında detaylı bir Türkçe kaynak bulamamam nedeni ile bu dökümanı oluşturmaya karar verdim.

Umarım herkes için faydalı bir kaynak olur.

Öncelikle IPSEC kullanma amacımızı hatırlayalım ;

- Güvensiz bir ortamda 2 kişinin güvenli bir şekilde konuşmasını sağlamak.
- Bu konuşma sırasında her 2 kişinin gerçekten doğru kişiler olmasının sağlanması ve ilgili konuşmanın 3. bir kişi tarafından dinlenmemesini/değiştirilmemesini sağlamak olarak da tanımlayabiliriz.

İşte tüm bunları sağlamak için kullandığımız protokolün adı IPSEC dir.

IPSEC tanım olarak IP katmanında (L3-Network katmanı olarak da söylenebilir) tüm IP iletişimini şifrelemek ve doğrulamak için kullanılan bir standarttır.

IPSEC iki şekilde karşımıza çıkar;

- ESP
- AH

### **ESP**

Esp yani Encapsulation Security Payload Doğrulama, Bütünlük-Değiştirilmeme ve Güvenilirlik işlemlerinin tümünü gerçekleştirir.

### **AH**

Authentication Header adından da anlaşılacağı gibi sadece Doğrulama ve Bütünlük-Değiştirilmeme işlemlerini sağlamakta fakat Güvenilirliği yerine getirememektedir.

AH nin ESP ye göre bir artışı vardır o da AH nin IP Başlık bilgisini de doğrulayabilmesidir.

(Konu hakkındaki ayrıntılı çizimler dökümanın sonunda incelenebilir.)

(Bknz.Şekil-6 ve Şekil-7 /Sayfa.10)

Burada geçen tanımları açmak gerekirse;

Doğrulama(authentication)

Her iki kişinin gerçekten doğru kişiler olması

Bütünlük-Değiştirilmeme (data integrity) Konuşmanın içeriğinin değişmeden karşıya ulaşması

Güvenilirlik (confidentiality/encryption) Konuşmanın 3. bir kişi tarafından duyulsa bile anlaşılması

Bu kavramlardan sonra sıra IKE kavramına geldi.

## **IKE**

IKE, IPSEC ile beraber kullanılan ve temelinde Diffie-Hellman anahtar deęişim yöntemini barındıran bir protokoldür.

IKE in 3 temel amacı bulunmaktadır.

1. 2 kişinin konuşmasını doğrulamak için bir çözüm sağlamak.
2. Yeni IPSEC oturumlarının oluşmasını sağlamak.(Yeni SA Security Association ler yaratmak)
3. Oluşmuş olan bağlantıları yönetmek.

IKE Phase 1 ve Phase 2 adı altında iki aşamadan oluşmaktadır.

### **IKE Phase 1**

Görevi IKE in nasıl korunacağına karar vermek ve korumaktır.

Phase 1 de iki şekilde gerçekleşebilir.

#### **Main Mode**

Phase 1 Main Mode olarak gerçekleştiğinde 3 aşamalı bir deęişim gerçekleşir.(Bknz.Şekil-3 Sayfa.7)

- İlk deęişimde öneriler üzerinde anlaşılmakta (doęrulama ve güvenilirlik için yöntemler)
- İkinci deęişimde Diffie-Hellman (Bknz.Şekil-2 Sayfa.7) kullanılarak dięer aşamalarda kullanılacak anahtarlar oluşturulmakta.
- Son aşamada ise karşı tarafın kimliği doęrulanmaktadır.

Bu olaylar Phase 1 bölümünde (Sayfa-5) ayrıntılı olarak açıklanmıştır.

#### **Aggressive Mode**

Phase 1 Aggressive Mode olarak gerçekleştiğinde ise daha az paket deęişimi olur.

İlk paket deęişiminde Diffie-Hellman public keyi,Identity paketi gibi tüm bilgiler aktarılır.

Bu paketi sadece onaylama paket izler.

Bu mode un Main Mode a göre dezavantajı güvenli bir kanal kurulmadan tüm deęişimlerin yapılmasıdır.

## IKE Phase 2

Görevi IPSEC in nasıl korunacağına karar vermektir.

Bu aşamada IPSEC sırasında Doğrulama ve Güvenilirlik adımlarında kullanılacak anahtarlar oluşturulmaktadır.

IKE in Doğrulama ve Güvenilirlik sırasında kullandığı yöntemler şu şekilde listelenebilir.

### IKE Güvenilirlik

- AES
- Blowfish
- 3DES
- DES

### IKE Doğrulama

- SHA1
- MD5

Burada araya girerek bu yöntemler hakkında bilgi vermek istiyorum.

Birçok kişinin bu yöntemler ve teknikleri hakkında çok fazla bilgisi bulunmamakta yada yanlış bilgileri mevcut.

Şifreleme alanında 2 farklı yöntem vardır.

1. **Simetric şifreleme (Secret key)** (Des,3Des,Aes vb)
2. **Asimetric şifreleme (Public key)** (Rsa,Diffie-Hellman,Sertifikalar)

Bu iki şifreleme yöntemlerinden Simetric şifreleme Asimetrik şifrelemeye göre daha hızlı bir yöntemdir.

**Simetrik şifreleme** olarak bahsedilen şey bir datayı şifrelemek ve bu şifreyi açmak için aynı anahtarın kullanılmasıdır.

**Asimetrik şifrelemede** ise datayı şifreleyen ve şifreyi açan anahtarlar farklıdır.

Simetric şifrelemede de iki yöntem vardır.

#### 1. Stream Cipher

Bu yöntemde veri bit bit okunabilir plain textden cipher text şekline dönüştürülür.

ipsec bir protoldur→ipsecbirprotokoldur→adnkehdyv

Sonrasında bu tek blok üzerinden şifreleme işlemleri gerçekleştirilir.

#### 2. Block Cipher

Bu yöntemde ise veri belli bloklara bölünür ve bu şekilde blok halinde cipher a dönüştürülür.

ipsec bir protokoldur→ipsec birpr otokl dur→hyart sndgv bnrtj fim

Sonrasında her blok ayrı ayrı şifrelenir.

[SSL](#), [PGP](#) ve [GPG](#) gibi sistemler ise hem simetrik hem de asimetrik şifreleme yöntemlerini bir arada kullanmaktadırlar.

Bu cipher sistemleri de kendi içlerinde işleyişlerine göre değişik isimler almakta.

Daha detay bilgiyi isteyenler araştırabilirler.

Simetric şifrelemede Des ve 3Des de kullanılan **Feistel Cipher**'ı;

$$i = 1, 2, \dots, n$$

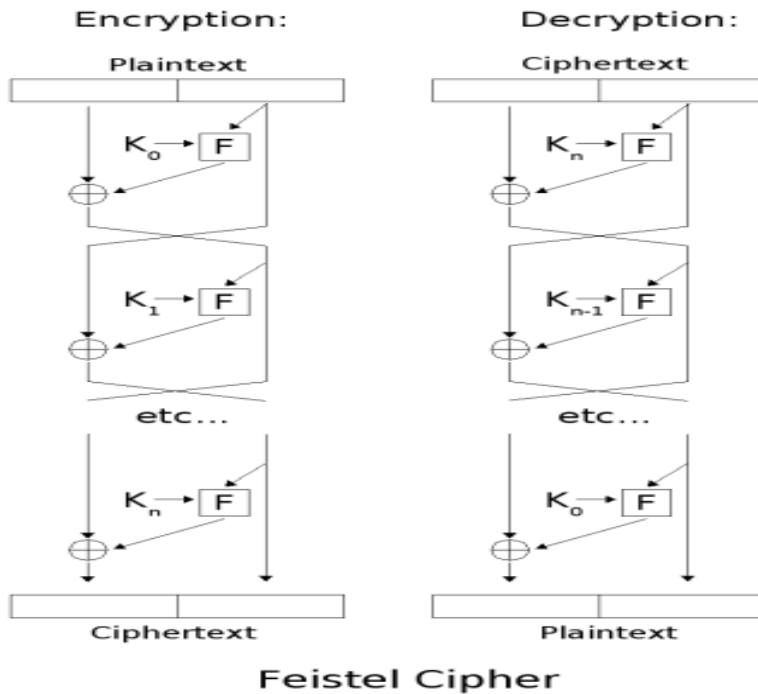
$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus f(R_{i-1}, K_i) \end{aligned}$$

$f$  fonksiyon ve  $K_i$  anahtar olmak üzere.

Bu durumda şifreli veri (ciphertext) =  $(L_n, R_n)$

Şifreyi çözmek için aynı fonksiyon ve anahtar kullanılır.

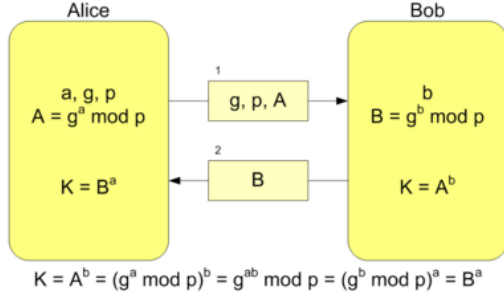
$$\begin{aligned} R_{i-1} &= L_i \\ L_{i-1} &= R_i \oplus f(L_i, K_i) \end{aligned}$$



**ŞEKİL-1 Feistel Cipher**

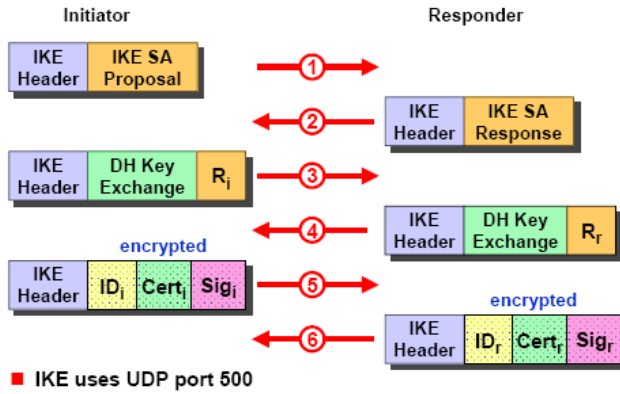
## Phase 1

### Diffie-Hellman



### ŞEKİL-2 Diffie-Hellman

#### Phase 1



### ŞEKİL-3 IKE Phase 1

IKE Phase 1 güvenli olmayan bir konuşma ile başlar. Bknz. Şekil-3

**1-2.** adımlar el sıkışma adımlarıdır. Burada her iki katılımcı el sıkışma işlemi gerçekleştirir. IKE başlığı ve SA Öneri bilgileri aktarılır.

→ HDR , SA

**HDR** = IKE başlığı (IKE header)  
**SA** = Öneri (Proposal)

**3-4** Şekil-3 de görüleceği gibi Diffie-Hellman bu aşamalarda devreye girer. Karşılıklı olarak IKE başlığı , KE (Key Exchange) Anahtar Değişimi ve  $R_i$ - $R_r$  (zamanla değişen rastgele sayı) bilgileri aktarılır.

→ HDR , KE ,  $N_i=R_i$

**KE** = Key Exchange ile  $G^a p$  ve  $G^b p$  Public değerler taşınır.

$G^{ab}$  Diffie-Hellman anahtarıdır ve  $KE(G^{ap}, G^{bp})$  public değerlerinden oluşturulur. Bknz. Şekil-2

$Prf$  = MAC/HMAC keyed-hash message authentication code SHA1/MD5

( $Prf \rightarrow$  HMAC in gerçekleştiği fonksiyon olarak tanımlanabilir.)

Bu aktarımla beraber artık  $G^{ab}$  Diffie-Hellman anahtarı her iki tarafın elinde oluşmuş durumdadır.

SKEYID olarak tanımladığımız ve bundan sonra hem IKE hem de IPSEC de kullanacağımız anahtarlarda bu aşamadan sonra oluşturulur.

$SKEYID = prf(\text{presharedkey}, R_i, R_r)$

Bu ilk anahtar ileride aşağıdakilerin oluşturulmasında kullanılır;

1. Phase 2 de **diğer** parametlerin yaratılması için anahtar  
 $SKEYID-d = prf(SKEYID, G^{ab}, \text{Cookie-a}, \text{Cookie-b})$

2. Phase 2 de **doğrulama** için kullanılacak için anahtar  
 $SKEYID-a = prf(SKEYID, SKEYID-d, G^{ab}, \text{Cookie-a}, \text{Cookie-b})$

3. Phase 2 de **güvenilirlik** için kullanılacak anahtar  
 $SKEYID-e = prf(SKEYID, SKEYID-a, G^{ab}, \text{Cookie-a}, \text{Cookie-b})$

**5-6** Bu işlemlerde artık bir önceki aşamalarda yaratılan anahtarlar kullanılarak şifreli ve doğrulamalı işlemler yapılıyor. IKE başlığımız artık şifreli ve ID mizin yanında bir de doğrulama için HASH bilgisi aktarılıyor.

$\rightarrow$  HDR\* , ID, Hash

$HASH = prf(SKEYID, G^{ap}, G^{bp}, \text{Cookie-a}, \text{Cookie-b}, SA, ID)$  SHA1/MD5

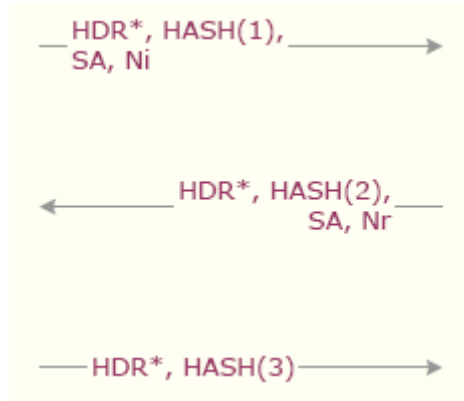
$HDR^* =$  Şifreli HDR (DES, 3DES, AES)

## Phase 2

Bu aşamada Phase 1 de biraz önce oluşturulan anahtar ve bilgiler kullanılır.

Her iki taraf Güvenilirlik ve Doğrulama konusunda anlaşır.

1.Öncelikle Quick Mode Exchange denilen olay gerçekleşir.Bu olay şifreli olarak yapılır. Şifreleme işlemi Phase 1 de oluşan anahtar ve bu anahtara katılan bazı ekstra parametreler ile yeni key oluşturulur ve şifreleme bu yeni key kullanılarak yapılır.



### ŞEKİL-4 IKE Phase 2 Quick Mode // PFS YOK

**Hash1-2** = prf (SKEYID-a,M-ID,SA,Nx)

**Hash3** = prf (SKEYID-a,M-ID,Ni,Nr)

**M-ID** = message id

**Ni-Nr**= bir kez kullanılan rastgele sayı

**Nx** = Ni veya Nr

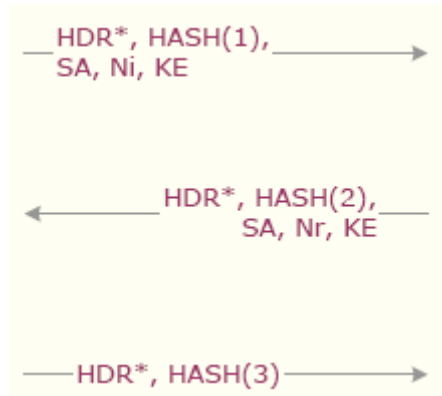
**SA** = öneri proposal

2.İpsec parametreleri konusunda anlaşılır

Bu anlaşma Quick Mode Exchange ile yaratılan SA kanalında olur.

Bu kanal bir süre sonra (expire/timeout) devre dışı kalır ve Quick Mode Exchange ile SA tekrar yaratılır.

3.PFS kullanılır ise SA kanalı yeniden yaratılması için Quick Mode un yenilenmesi yetmez ve Diffie-Hellman ile baştan yeni anahtarlar üretilir.



### ŞEKİL-5 IKE Phase 2 Quick Mode // PFS VAR

## ESP AH

### ESP (Encapsulating Security Payload)

ESP protokolü hem doğrulama hem de güvenilirlik için kullanılabilir. Bunun yanında sadece doğrulama veya sadece güvenilirlik için de kullanılabilir.

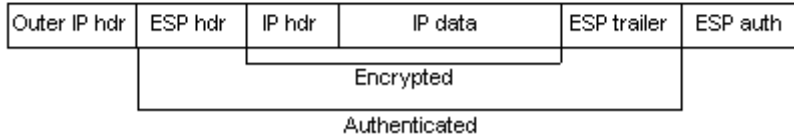
Original IP packet



ESP in transport mode



ESP in tunnel mode



### ŞEKİL-6 ESP

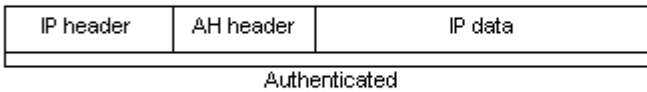
### AH (Authentication Header)

AH ise veriyi doğrulamak için kullanılan bir protokoldür. AH ise IP paketindeki data için şifreli bir hash fonksiyonu kullanarak MAC bilgisi elde eder. Bu MAC verisi orjinal paket ile beraber karşı tarafa yollanır ve alıcı kişinin orjinal verinin bütünlüğünün değiştirilmediğini anlamasını sağlar.

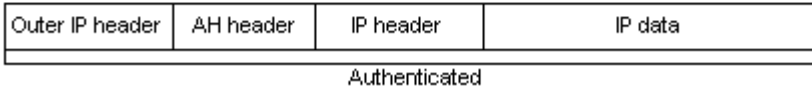
Original IP packet



AH in transport mode



AH in tunnel mode



### ŞEKİL-7 AH

# DIFFIE-HELLMAN

