

CHAPTER - 8

Network Security

(Ağdaki Güvenlik)

- Networkteki Güvenlik ;

1) Gizlilik ; bir mesajın içeriğini sadece gönderici ve alıcı paylaşmalı. Bu gizliliğin olması için şifreleme kullanılır.

2) Kimlik Doğrulama ; gönderici ve alıcı birbirlerinin olduğunu doğrulamak isterler.

3) Mesaj Bütünlüğü ; gönderici ve alıcı gönderilen mesajın değişmeden yada bozulmadan karşı tarafa geçmesini isterler.

4) Kullanılabilir ve Uygunluk

Friends and Enemies: Alice, Bob, Trudy

- Bob ve Alice güvenli iletişim kurmak istiyor
Trudy bağlantıyı kesebilir, mesajları değiştirebilir.
- Bob ve Alice kimler olabilir? (GÜVENLİK ÖNEMLİ OLANLAR)
 - * biz, browser ve serverlar, DNS serverları (tüm IP adreslerini sakladığımız yer)
 - online bankacılık yapanlar, routerlar
- Kötü adamlar (Trudy gibi) neler yaparlar?
 - * dinleme, taklit etme, kırım, birinin yaptığı işi üstlenme, hizmet reddi
- * İnternet tamamen karşılıklı güvene dayanarak oluşturulmuştur.
- kötü yazılımlar, trojanlar, virüsler, botnet ve D.Dos atakları, wormlar bu güvenliğe karşı olanlardır.

Şifreleme Dili

Alice mesaj oluşturdu ve bunu şifreleyecek

Şifreleme anahtarı K_A

mesaj + $K_A \xrightarrow{\text{ciphertext}}$ K_B + mesaj

K_A : encryption anahtarı (şifreleme anahtarı)

K_B : decryption anahtarı (şifre çözme anahtarı)

m : mesaj (şifresiz)

ciphertext: K_A ile şifrelenmiş mesaj

$$m = K_B(K_A(m))$$

Substitution şifreleme:

Var olan karakterin yerine başka bir karakter kullanmak.

* monoalphabetic cipher:

plaintext: abc...xyz

ciphertext: mnb...ewq

Aynı alfabeyle karşı 1 şifreli alfabe

* polyalphabetic şifreleme

- 1'den çok alfabeyle şifrelemek için kullanılır.
- n tane monoalfabe var. ($M_1, M_2, \dots, M_n$)
- cycling pattern: şifreleme yaparken hangi alfabeyle izleyeceğim $n=4$ $M_1, M_3, M_4, M_3, M_2; M_1, M_3, M_4, M_3, M_2$

dog: d'yi M_1 'den; o'yu M_2 'den; g'yi M_4 'ten

Anahtar: n chipper ve cyclic pattern

Güvenli e-mail

Hem gizlilik, hem kimlik doğrulama

SSL

Tüm TCP uygulamaları için kullanılır. API görevi görür.

SSL yapısının içinde

✓ handshake

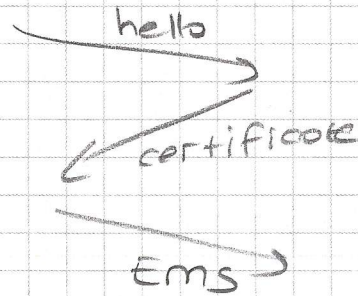
Alice ve Bob kendi sertifikalarını birbirleriyle paylaşırlar.

✓ anahtar üretimi

✓ data transferi

✓ connection closure

Simple Handshake



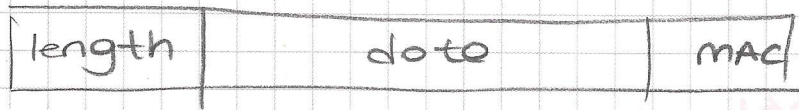
Anahtar Üretimi

Birden çok anahtar kullanılır.

✓ ke, ks, mc, ms > 4 anahtar.

Keyler bir function kullanılarak üretilir.

Data Records Transmit

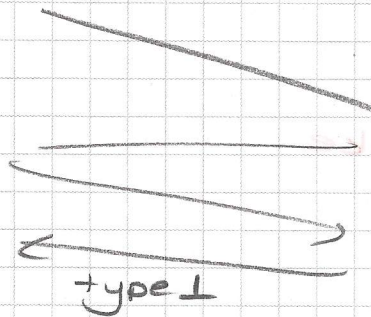


- Sequence number kullanılır. MAC'in içine data ile birlikte seq. number yerleştirilir.

$$MAC = MAC(M_x, sequence || data)$$

- Bağlantı engellenmesin diye data type alanı oluşturur. type 1 → bağlantı kopatılarak

TOY SSL:



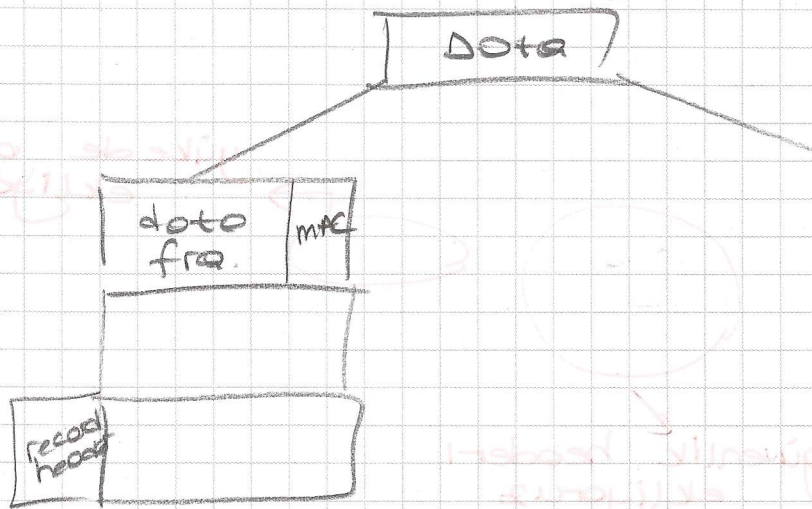
- * Client ve server tarafı farklı şifreleme algoritmalarını destekleyebilir. Ya da daha önceden aynı algoritmayı kullanacaklarına karar verirler.

Real SSL : Handshake

- 1) Server out
- 2) Negotiation
- 3) _____
- 4) _____

SSL Record Protocol

Data lar fragmentationlara ayrilmistir.



Key üretimi

Nounce ve pre-master secret bu noktalarla oluşturulur.

VPNs

(Sanal Özel Ağlar)

Bir kurum içinde tüm bilgi payloadlarını gizli (kendi içinde) yapmak isteyebilir,

Bunun için;

- VPN yapılarını oluşturmuslardır.

Aynı kurumun birimleri, birbiri ile iletişim kurmak isterlerse

IP header + payload = bilgisayarın routers

↳ TCP ya da UDP

IP header + IPsec header + secure payload = routerden diğer internete

güvenlik headeri ekliyoruz

yüke de güvenlik ekliyoruz.

IPsec'in Sağladıkları

- Data bütünlüğü
- Origin auth.
- Replay - - -
- confiden

IPsec - tunneling mode

IPsec routerden başlar

(Routerden
routera
(Yada routerden
hosta gider)

IPsec - transport mode

IPsec hostta başlar.

2 PROTOKAL

AH: Source auth. sağlar. Data bütünlüğü
Gizlilik sağlamaz.

ESP: Hepsini sağlar.

Security associations (SAs)

Veriyi göndermeden önce sonal bağlantı kurulur gönd. ve alıcı arasında. Bu bağa SA denir.

- Veri gönderimi tek yönlüdür.
- Her iki taraf göndericekse ayrı ayrı SA kurulur.
- TCP bağlantı durumunu soklar, IP yapış. da sokulması IPsec yapısı bağlantı durumunu soklar.

SA from L_1 to L_2

Bir SA bağlantısında hangi bilgiler tutulur.

- SPI
- SA'nın orjinal arayüzü (L_1 'in IP'si)
- Hedefin IP'si
- Şifreleme t1p1
- Şifreleme monitör1
- Kimlik doğrulama monitör1

SAD

SA'lar bir database'in içinde tutulur yeni SAD'nin Endpointler SA'ların durumunu SAD'de tutarlar.

IPsec datagramlarını gönderirken R1 SAD'a ulosur ve hangi işleni yapacağını söyler.

- R1 R2'ye SA oluşturduğunda hem R1'in hem R2'ni SAD'inde tutulur.

IPsec Datagram

new IP header	ESP hdr	original IP head	original IP datagram payload	ESP trailer	ESP auth
---------------------	------------	---------------------	---------------------------------	----------------	-------------

yeni yeni daha önceden vardı

Anahtarları kullanarak bu bölüm şifrelenir (SA'da)

encilode

SPD (Security Policy Database)

* SPD'nin içinde; bana gelen bir datagramla ilişki olarak ben ne yapacağım.

* SAD bana gelen datagramla olan işlemleri Nasıl yapacağım

WEP (wired equivalent Privacy)

- Kablosuz bağlantıda güvenlik

Block chipper değil stream chipper yapısı kullanılır.

Her bir paket ayrı ayrı şifrelenir.

Bu bağımsızlık için sadece key'i kullanmıyoruz.

IV dediğimiz kod her paket için yenilenir.

WEP encryption

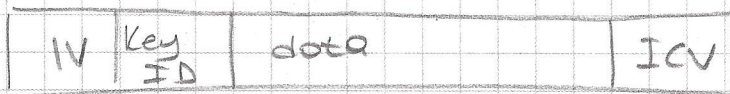
- ICV datası (data bütünlüğünü kontrol eder)

- Her bir tarafta shared key var (104 bit)

- Gönderici IV dediğimiz başlangıç vektörünü

oluşturur ve shared key'in arkasına ekler

- Bunlara bir de Key ID eklenir.



MAC payload

shared key
+ IV

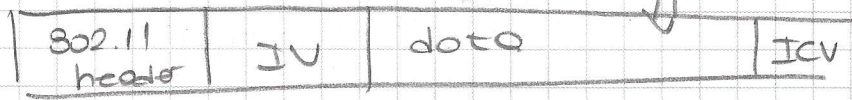
$K_s + IV = k_1 \quad k_2 \quad \dots$

Original data = $d_1 \quad d_2 \quad \dots \quad \text{CRC}$
+ CRS

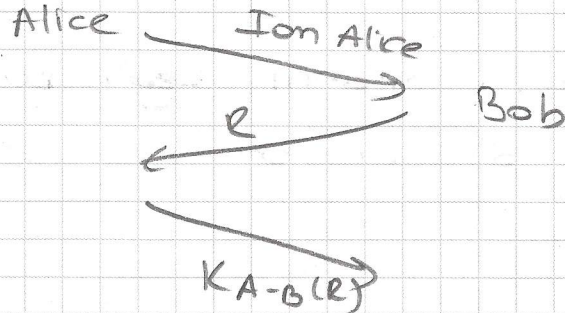


Bunları XOR'luyoruz.

$x_1 \quad x_2 \quad x_3$



Nonce: Sana konuştüğüm kişi sen misin bilgisini
veren



key ile gönderir
Alice Nonce'i şifreleyip gönderir

Web Authentication

Host AP'ye out. isteği gönderir. AP'de
nonce gönderir. Host nonce'i şifreleyip gönderir.

802.11 - şifresi kırılabilir mi

IV 24 bit ve her frame için yeni oluşturulur. Bu durum kullanılan şifreleri birgün mutlak olarak tekrar kullanmak durumundadır. Trudy bu durumu kullanabilir. Bunu nasıl önleriz?

- ✓ Daha güçlü şifrelene yapılır
- ✓ Auth. server'ı AP'den farklı bir server üzerinden yapılabilir

Bu yapıyı öcarsak;

Kimlik doğrulama işlemini AS'den yaparız.

- Client güvenlik yapılarını keşfeder.
- AP ile kimlik doğrulama için bağlanma gerçekleştirir.
- STA ve AS'de master key üretilir.
- STA ve AS bu master key'i kullanarak 2'side PMK oluşturur.
- Server ürettiği PMK'yı AP'ye gönderir.
- Client ve AS ellerindeki PMK key'i ile kimlik doğrulama işleminin gerçekleştirildiğini görür ve iletişime geçerler.

(AS)
* MK (master key) : Client ve server arasındaki ilk paylaştığımız key. Daha sonra mk'yi kullanarak AS ve client bir şifre daha oluşturur. Bu şifreye PMK denir. AP üzerinden bu şifreler doğrulanır. Bu üçü TK şifresini oluşturur.

EAP: Bu yapıyı yürüten protokol.

→ EAPol

Client ve AP arasında kablosuz. AP ve AS arasında kablolu yapı var.

RADIUS protokolü.

Firewalls (Güvenlik Duvarı)

Bizi ana internetten izole edebilen, kendi ağımızı denetlememizi sağlar.

Neden güvenlik duvarı var?

- ✓ prevent denial of service attacks
- ✓ prevent illegal modification/access of internal data
- ✓ allow only authorized access

3 tip güvenlik duvarı var.

- Stateless packet filtering (Durumu kontrol etmez)
Durum bilgisi tutmaz. (Elle izlen yapılır)
Router kaynak ve hedef IP'sine göre, ICMP
ye göre, vb. bitlere bakarak paketlere
geçip geçme diyebilir.

Stateless pack. filtering example;

Ex 1: UDP kullanılmışsa ya da dest port: 23
se paketleri geçirme.

ACCESS CONTROL LIST

✓ Hangi kısımlar var?

- action

- source address, dest. ad., protocol...

Statefull Packet Filtering

Her TCP bağlantısının durumu izlenir. Durum
kontrol edilir. Kontrol tablosuna "check connection"
kısımı ilave edilir.

= Application Gateways =

Gateway üzerinden bağlantı kurulur. Tüm uygulama programları için gateway'e ihtiyas vardır. Karşılıklı olarak kimlik doğrulama bu gateway üzerinden gerçekleşir.

Limitations of firewalls and gateway

İstemcinin hangi gatewayi kullanacağını bilmesi gerekir. UDP ile gelen paketleri ya geçirir ya geçirmez. Bozillerini geçirme diye birşey yok.

trade off: hem güvenliği arttırmak hem iletisimi art. yok. Güvenliği ↑ iletisimi azaltıyoruz.

INTRUSION DETECTION SYS.

Sınırları azaltmak ya da arttırmak için kullanılır.

- Paket filtreleme işlemi gerçekleştirilir. TCP yada UDP'nin headerlarına bakılarak IDS'yi kullanıyorsa, paketlerin contentine bakar. Örn; bir kelime. O kelime pakette geçiyorsa o pakete geçiş vermez.

Paketlerin içeriğine bakar.

→ IDS , otığı poketlerin kaynğını sorgular.
Tüm dropoldığımız poketler aynı kaynaktan
geliyor olabilir. İstatistik yapar ve bu
kaynğı bulur.

✓ Farklı yerlerde farklı şekilde kullanabilir.