Bilgisayar Programcılığı
Uzaktan Eğitim Programı

e-BİLG 121 AĞ TEKNOLOJİLERİNİN TEMELLERİ

Öğr. Gör. Bekir Güler

E-mail: bguler@fatih.edu.tr

13. Hafta: Ağ güvenliği II

8.5 Güvenli soket katmanı: SSL

8.6 Ağ katmanı güvenliği: IPSec

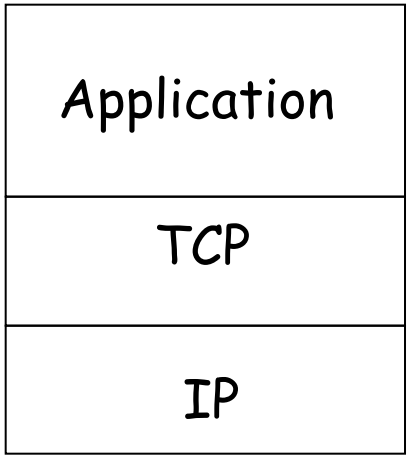
8.7 Kablolu yerel ağda güvenlik

8.8 Güvenlik duvarı ve saldırı tespit sistemleri

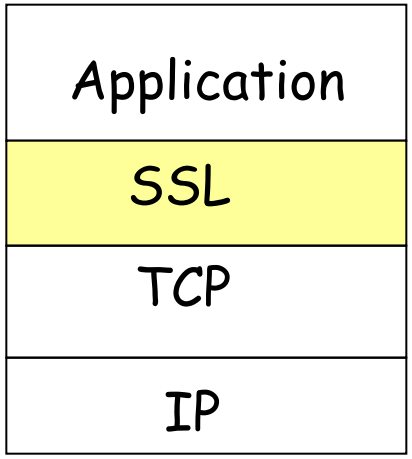
8.5 Güvenli soket katmanı (Secure Sockets Layer-SSL)

- Yaygın kullanılan güvenlik protokolü
  - Hemen hemen tüm web tarayıcı ve sunucular tarafından desteklenir
  - https
  - SSL üzerinden her yıl milyarlarca $ para harcanır
- Netscape tarafından 1993 yılında tasarlandı
- Sağladıkları:
  - Gizlilik
  - Bütünlük
  - Kimlik doğrulama
- Hedefleri:
  - Web e-ticaret işlemleri
  - Şifreleme (özellikle kredi kart numaraları)
  - Web sunucu kimlik doğrulaması
- Tüm TCP uygulamaları için kullanılabilir olması

SSL ve TCP/IP



Normal uygulama



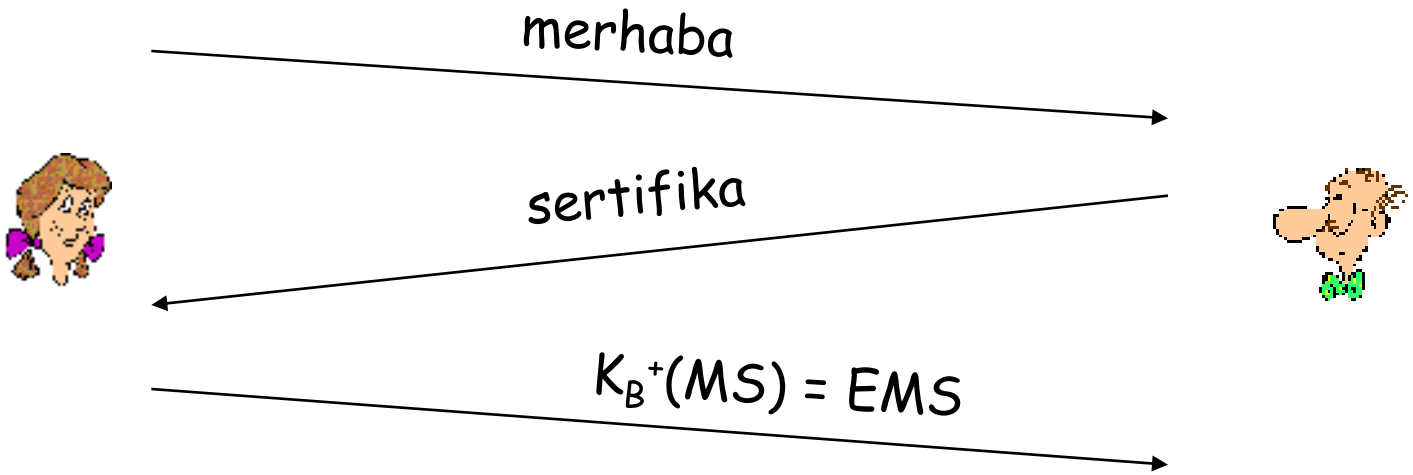
SSL ile uygulama

- SSL, uygulamalara application programming interface (API) sağlar
- C ve Java SSL kütüphanelerinde/sınıflarında kullanıma hazır

SSL: Basit güvenli kanal

- El sıkışma: Ayşe ve Basri kendi sertifika ve özel anahtarlarını kullanarak birbirlerinin kimliklerini doğrulamak ve gizli bilgileri değiştirmek istiyorlar
- Anahtar türetme: Ayşe ve Basri anahtarlar türetmek için paylaşılan gizli kodu kullanır
- Veri transferi: Aktarılacak veriler bir dizi kayıta ayrılır
- Bağlantıyı kapatma: Bağlantı güvenli bir şekilde kapatılır

El sıkışma



- MS = master secret
- EMS = şifreli master secret

Anahtar türetmek

- Aynı anahtarı birden çok şifreleme için kullanmak kötüdür
  - Mesaj doğrulama kodu ve şifreleme için farklı anahtarlar kullanılır
- 4 anahtar:
  - K_c = İstemciden sunucuya gönderilen veri için şifreleme anahtarı
  - M_c = İstemciden sunucuya gönderilen veri için mesaj doğrulama kodu anahtarı
  - K_s = Sunucudan istemciye gönderilen veri için şifreleme anahtarı
  - M_s = Sunucudan istemciye gönderilen veri için mesaj doğrulama kodu anahtarı
- Anahtarlar KDF(key derivation function) ile elde edilir
  - Master secret ve bazı ek rasgele veriler kullanılarak anahtarlar elde edilir

Veri kayıtları

- Bit akışı bir dizi kayıta bölünür
  - Her kayıt mesaj doğrulama kodu MAC taşır
  - Alıcı mesajı aldığında her kayıt üzerinde işlem yapabilir
- MAC ve verinin birbirinden ayrılması gerekir
  - Değişik uzunlukta kayıt kullanılabilir

Bir şifreleme algoritmasını seçmek

- İstemci ve sunucu farklı şifreleme algoritmaları destekleyebilir
- İstemci ve sunucu veri iletimi öncesinde belli bir şifreleme algoritması üzerinde anlaşması gerekir

SSL'de yaygın kullanılan simetrik şifreler

- DES – Data Encryption Standard: blok
- 3DES – 3 kat daha güçlü: blok
- RC2 – Rivest Cipher 2: blok
- RC4 – Rivest Cipher 4: bit akışı

Ortak anahtar şifrelemesi

- RSA

El sıkışma (1)

1. Sunucu kimlik doğrulaması
2. Bir şifreleme algoritmasında anlaşma
3. Anahtarları oluşturmak
4. İstemci kimlik doğrulaması (opsiyonel)

El sıkışma (2)

1. İstemci desteklediği şifreleme algoritmalarının listesini gönderir
2. Sunucu listeden seçer ve geri gönderir
3. İstemci sertifikayı onaylar, sunucunun ortak anahtarını alır, pre_master_secret üretir, sunucu ortak anahtarı ile şifreler ve sunucuya gönderir
4. İstemci ve sunucu bağımsız olarak şifreleme ve mesaj doğrulama kodunu hesaplar
5. İstemci tüm karşılıklı mesajlar için bir mesaj doğrulama kodu gönderir
6. Sunucu tüm karşılıklı mesajlar için bir mesaj doğrulama kodu gönderir

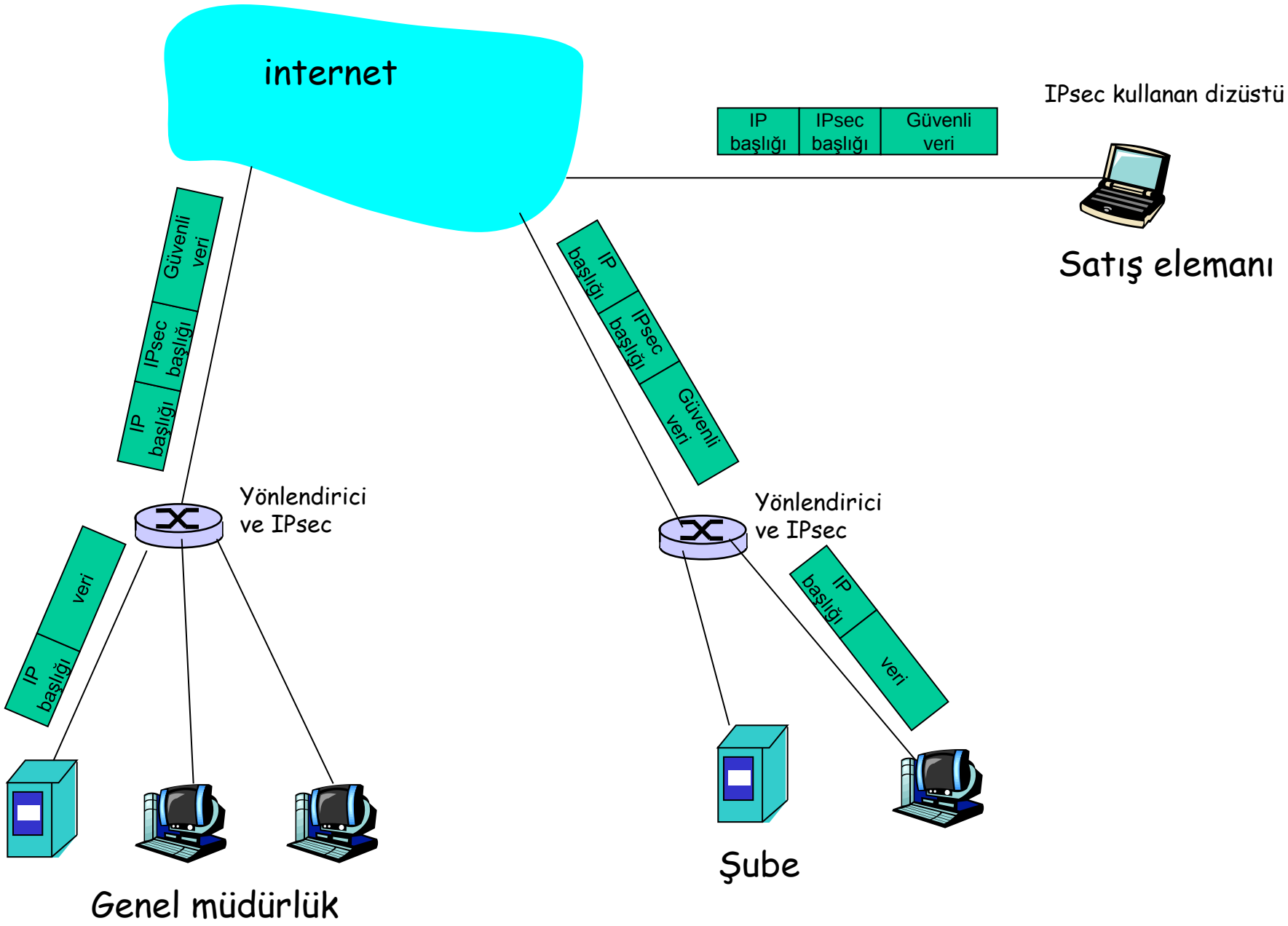
8.6 Ağ katmanı güvenliği: IPSec

- Gönderen datagram içindeki veriyi şifreler. Datagram içinde:
  - TCP segment, UDP segment, ICMP mesajı olabilir
- Göndericiden alıcıya gönderilen tüm veriler gizli olmalıdır:
  - Web sayfaları, e-posta, P2P dosya transferi, TCP SYN paketleri ve benzerleri

Sanal özel ağlar (Virtual Private Networks-VPNs)

- Kurumlar güvenlik için özel ağlar isterler
  - Ayrı yönlendirici, bağlantı ve DNS yapısı kurulursa pahalı olur
- Ekstra bir harcama yapmadan internet üzerinden sanal özel ağlar kurulabilir
  - İletimden önce yerel ağdaki veri şifrelenerek internete gönderilir

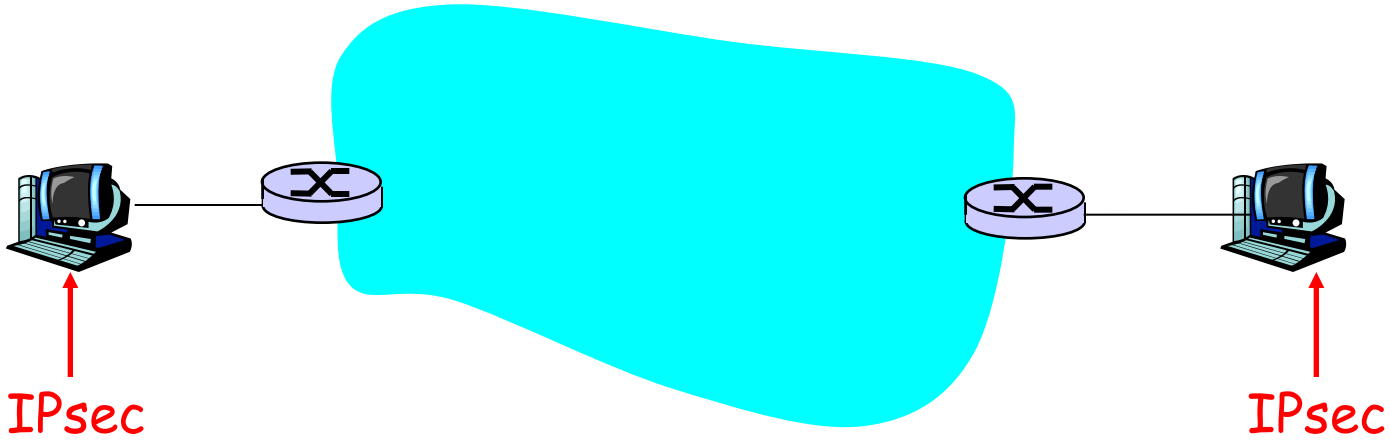
Sanal özel ağ (VPN)



IPsec hizmetleri

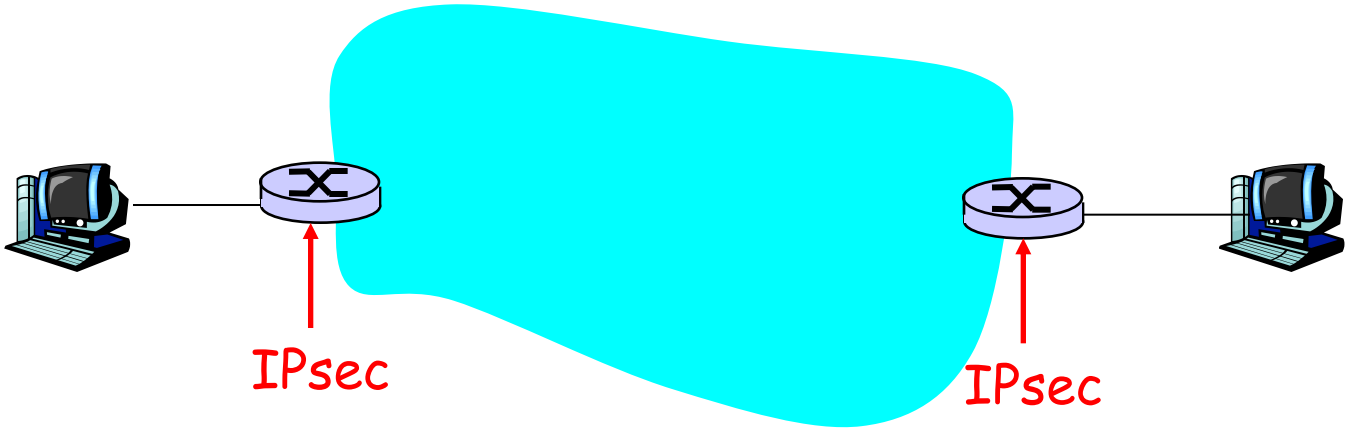
- Veri bütünlüğü
- Kimlik doğrulama
- Saldırıları engelleme
- Gizlilik

IPsec iletim modu (1)



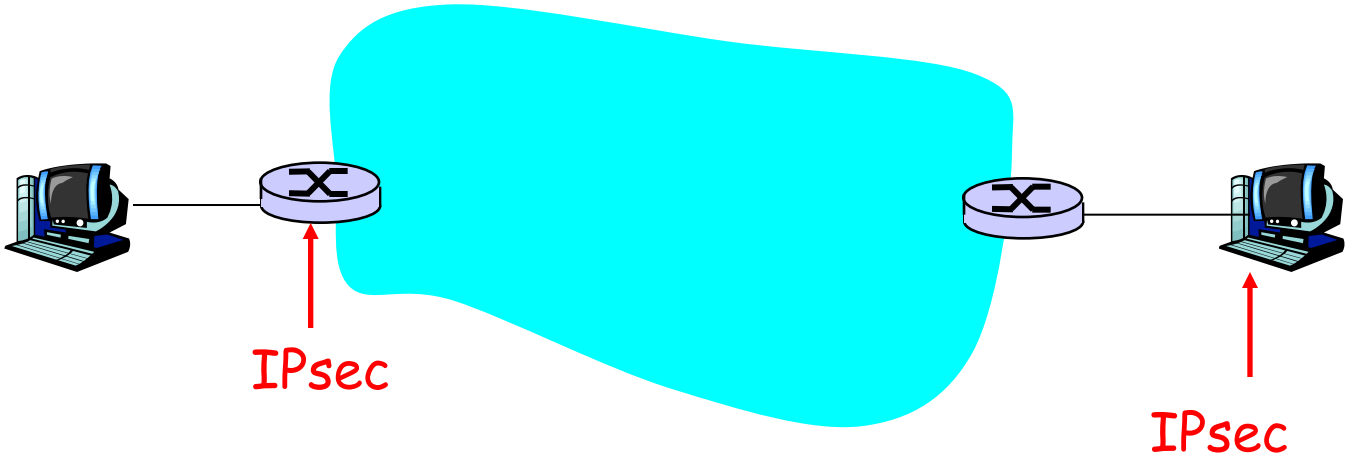
- IPsec datagram'ları bilgisayarlarda alışverişi yapılır

IPsec tünel modu (2)



- IPsec, yönlendiricilerde uygulanır.

IPsec tünel modu (3)



- IPsec yönlendirici ve bilgisayarda uygulanır

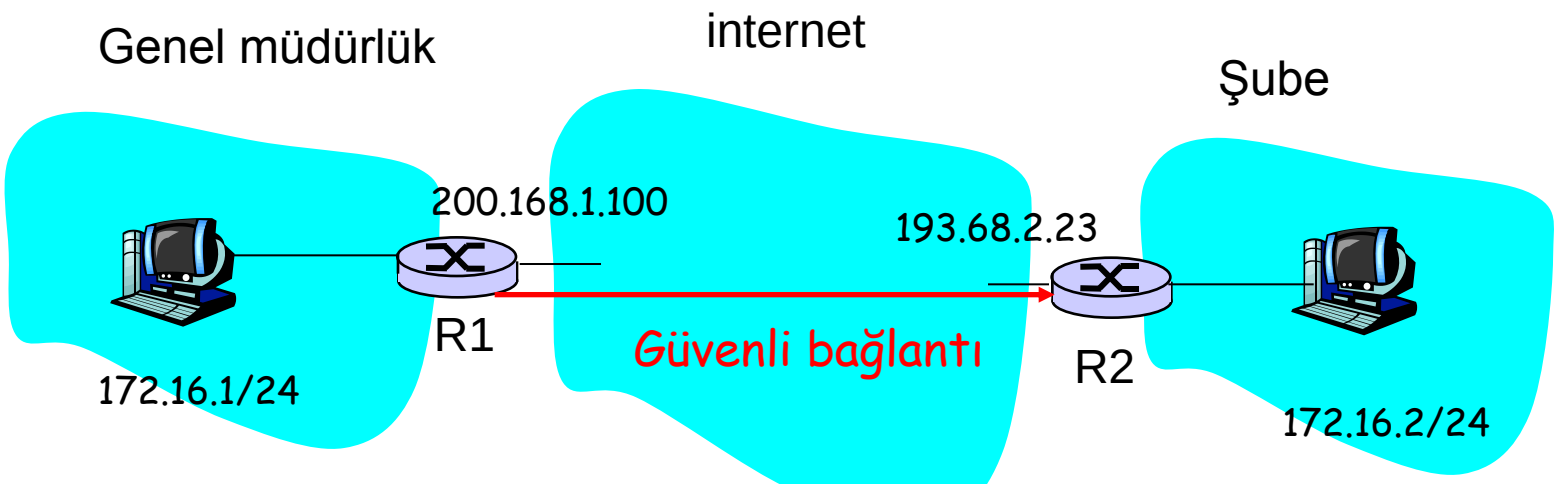
2 protokol

- Authentication Header (AH) protokol
  - Kaynağın kimlik doğrulaması ve veri bütünlüğü sağlar
- Encapsulation Security Protokol (ESP)
  - Kaynağın kimlik doğrulaması, veri bütünlüğü ve gizlilik sağlar
  - Yaygın olarak kullanılır

Güvenli bağlantı

- Veri göndermeden önce, gönderen ve alıcı arasında sanal bağlantı kurulur
- Güvenli bağlantı tek yönlüdür.
- Hem gönderen hem de alıcı güvenli bağlantı ile ilgili durum bilgilerini saklarlar
  - TCP bağlantısında da durum bilgileri saklanırdı
  - IPsec de bağlantılı bir protokoldür

R1'den R2'ye güvenli bağlantı



R1 güvenli bağlantı için aşağıdaki bilgileri saklar

- Güvenli bağlantı için 32 bitlik tanıtıcı
- Güvenli bağlantının kayak arabirimi (200.168.1.100)
- Güvenli bağlantının hedef arabirimi (193.68.2.23)
- Kullanılan şifreleme türü (örneğin, 3DES)
- Şifreleme anahtarı
- Bütünlük denetim türü (örneğin, HMAC)
- Kimlik doğrulama anahtarı

İnternet anahtar değişimi

- IPsec güvenli bağlantıda anahtarları el ile değiştirmek pratik değildir. Yüzlerce bağlanan kullanıcı olabilir

Örnek güvenli bağlantı

SPI: 12345
Source IP: 200.168.1.100
Dest IP: 193.68.2.23
Protocol: ESP
Encryption algorithm: 3DES-cbc
HMAC algorithm: MD5
Encryption key: 0x7aeaca…
HMAC key:0xc0291f…

- Anahtarları pratik değiştirmek için *IPsec IKE (Internet Key Exchange) kullanılır*

IKE: PSK ve PKI

- Kimlik doğrulaması aşağıdaki 2 yolla yapılabilir
  - pre-shared secret (PSK) veya
  - PKI (pubic/private keys ve certificates).
- PSK'da, iki tarafta ta gizli kodla başlar:
  - Sonra birbirlerinin kimliklerini doğrulamak ve IPsec güvenli bağlantı oluşturmak için IKE çalıştırılır
- PKI'de, iki tarafta ortak/özel anahtar ve sertifika ile başlar:
  - Birbirlerinin kimliklerini doğrulamak ve IPsec güvenli bağlantı için IKE çalıştırılır
  - SSL bağlantısına benzer.

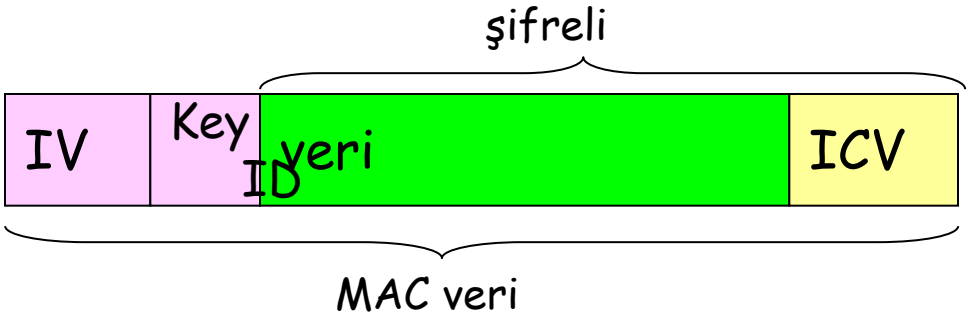
8.7 Kablosuz yerel ağda güvenlik

WEP (Wired Equivalent Privacy) tasarım hedefleri

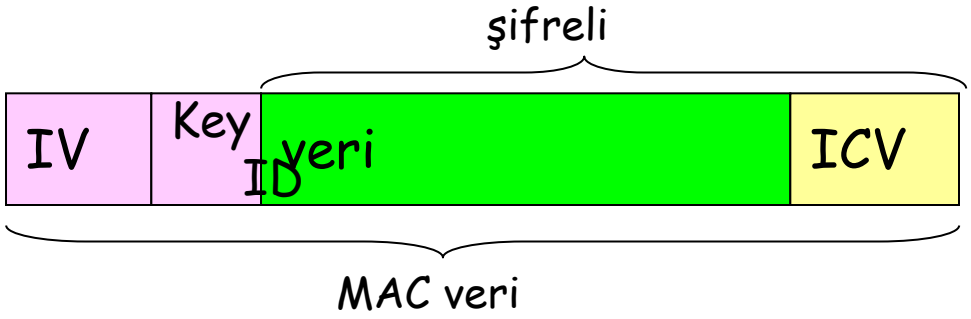
- Simetrik anahtar şifrelemesi
  - Gizlilik
  - Kimlik doğrulaması
  - Veri bütünlüğü
- Her paket ayrı şifrelenir
  - Şifreli paket ve anahtar verilirse şifre çözülür
- Verimli
  - Donanımsal ve yazılımsal uygulanabilir

WEP şifreleme

- Gönderen, verinin bütünlük denetim değerini (Integrity Check Value-ICV) hesaplar
- İki tarafta ta paylaşılan 104 bitlik paylaşılan anahtar vardır
- Gönderen, 24 bitlik başlangıç vektörü (initialization vector-IV) oluşturur ve anahtara ekler. Toplamda 128 bitlik anahtar elde edilir
- Gönderen, ayrıca 8 bitilik keyID ekler
- 128 bitlik anahtar sayı üreticisine girişi yapılarak keystream elde edilir
- Veri ve ICV, RC4 ile şifrelenir:
  - keystream ve veri & ICV XOR işleminden geçirilir
  - IV & keyID değerleri şifreli veriye eklenerek veri oluşturulur
  - Veri, 802.11 frame içen konur



WEP şifre çözme



- Alıcı, IV'yi çıkarır
- IV ve paylaşılan gizli anahtar rasgele sayı üreticisine girişi yapılır, keystream elde edilir
- Veri + ICV şifresini çözmek için keystream ve şifreli veriye XOR işlemi uygulanır
- ICV ile verinin bütünlüğü doğrulanır

802.11 WEP şifrelemesini kırma

Güvenlik açığı:

- 24 bitlik IV, bir IV bir frame için, -> Sonunda IV'ler yeniden kullanılıyor
- IV düz metin olarak aktarılıyor -> yeniden kullanılan IV tespit edilebilir

802.11i: Geliştirilmiş güvenlik

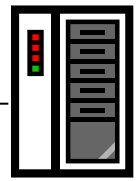
- Daha güçlü şifreleme sağlar
- Anahtar dağıtımı sağlar
- Erişim noktasından farklı olarak kimlik doğrulama sunucusu kullanır

802.11i: 4 aşaması

STA:
istemci

Erişim noktası

Kablolu ağ



Kimlik doğrulama
sunucusu

1 Güvenlik özelliklerini öğrenmek

2 İstemci ve sunucu karşılıklı olarak kimliklerini doğrular,
Beraber Master Key (MK) üretirler

3 İstemci Pairwise Master
Key (PMK) türetir

3 Sunucu aynı PMK üretir,
erişim noktasına gönderir

4 İstemci ve erişim noktası PMK kullanarak
Temporal Key (TK) türetir.
TK mesaj şifreleme ve bütünlüğünde kullanılır

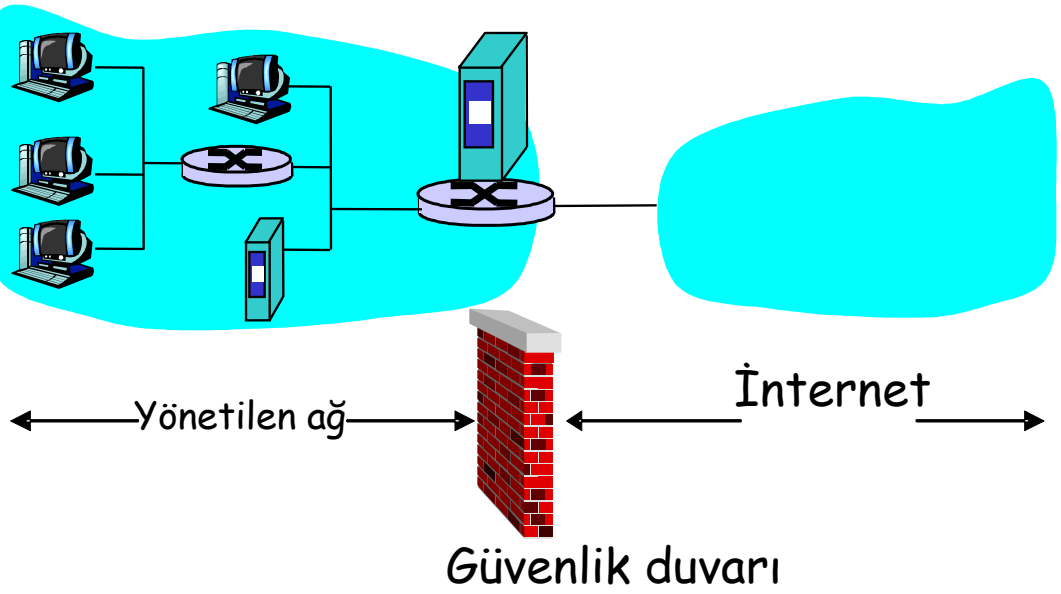
EAP: extensible authentication protocol

- EAP: İstemciden mobil istemciye kimlik doğrulama sunucu protokolüdür
- EAP, ayrı bağlantılar üzerinden gönderilir
  - Mobilden erişim noktasına (EAP, LAN üzerinden)
  - Erişim noktasından kimlik doğrulama sunucusuna (RADIUS, UDP üzerinden)

8.8.1 Güvenlik Duvarı (Firewall)

Güvenlik Duvarı

Kurumsal ağ ile interneti izole eder, bazı paketlerin geçicine izin verirken diğerlerini engeller



Güvenlik duvarı

Hizmeti engellemeye yönelik saldırılar:

- SYN seli: Hacker, sunucuya birçok sahte TCP bağlantısı kurar, gerçek bağlantılar için kaynak kalmaz

İç verilerin, yasadışı değişimini/erişimini engellemek

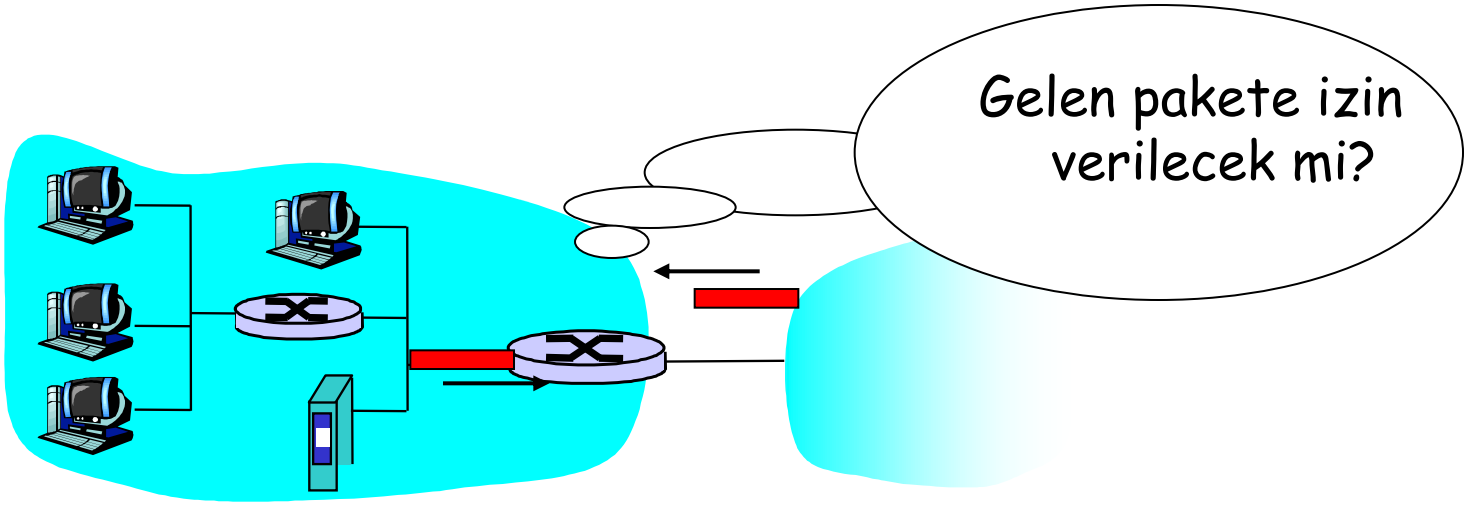
- Örneğin, Google web sayfasının başka bir şeyle değiştirilmesi

İç ağa sadece yetkili kullanıcıların girişine izin vermek (kimlik doğrulaması yapılmış kullanıcı ve bilgisayarlar)

3 tür güvenlik duvarı:

- Durum bilgisi olmayan paket filtreleri
- Durum bilgisi olan paket filtreleri
- Uygulama ağ geçitleri

Durum bilgisi olmayan paket filtreleri



- İç ağ, internete yönlendirici güvenlik duvarı ile bağlıdır
- Yönlendirici paketleri iletmek veya atmak için tek tek filtreler:
  - Kaynak IP adresi, hedef IP adresi
  - TCP/UDP kaynak ve hedef port numaraları
  - ICMP mesaj türü

Durum bilgisi olmayan paket filtreleme örnekleri

Kural	Güvenlik duvarı ayarı
Web erişimini engelleme	Dışarı herhangi bir IP adresine, port numarası 80 olan paketleri at
Kurumun web sunucusu dışındaki gelen TCP bağlantılarını engelle	IP adresi 130.207.244.203, port 80 olan gelen TCP SYN paketlerini izin ver diğerleri at
Web radyolarının kullanımını engellemek	DNS ve yönlendirici broadcast dışındaki gelen UDP paketlerini at
DoS saldırılarına karşı ağınızı engellemek	Broadcast adreslerine (örneğin, 130.207.255.255) giden tüm ICMP paketlerini at

Erişim kontrol listesi

- Kurallar paketlere yukarıdan aşağıya doğru uygulanır

İşlem	Kayak adres	Hedef adres	protokol	kaynak port	hedef port	bayrak biti
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Durum bilgisi olan paket filtreleme

- Durum bilgisi olmayan paket filtrelemeyi kullanmak zordur
- *Durum bilgisi olan paket filtreleme:* Her TCP bağlantısının durumunu izler
  - Bağlantının kurulumunu (SYN) ve kapatılmasını (FIN) izler. Giden ve gelen paketlerin bir anlamı olup olmadığını belirleyebilir
  - Güvenlik duvarında zaman aşıma uğrayan aktif olmayan bağlantıları kapatır

Durum bilgisi olan paket filtreleme

- Paketler kabul edilmeden önce erişim kontrol listesinin artması bağlantı durumlarının kontrol edilmesi gerektiğini gösterir

İşlem	Kaynak adres	Hedef adres	protokol	Kaynak port	Hedef port	bayrak biti	Bağlantı kontrolü
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

8.8.2 Saldırı tespit sistemleri (Intrusion detection systems-IDS)

- Paket filtreleme:
  - Sadece TCP/IP başlıkları üzerinde çalışır
  - Korelasyona bakmaz
- *Saldırı tespit sistemleri*
  - *Paketi derinlemesine inceler:* Paket içeriklerine bakar (örneğin, bilinen virüs ve saldırı isimleri için paket içeriğini kontrol eder)
  - Paketler arasındaki korelasyonu inceler
    - port taraması
    - DoS saldırısı

Saldırı tespit sistemleri

- IDS sensörler ile farklı noktalarda farklı denetimler yapılır