* Şifrelenmiş veri iletim sistemleri.

* SSL Teknolojisi.

* Apache sunucusu ile güvenli HTTP bağlantıları.

* Bir gerçek yaşam örneği : “LKD SSL Sunucusu”

Berk Demir <berk@linux.org.tr>

Linux Kullanıcıları Derneği

İçerik :

- HTTP protokolüne genel bir bakış.
- HTTP protokolü sebepli ortaya çıkan güvenlik açıkları.
    - Güvenlik sorunlarına çözümsel yaklaşımlar.
- SSL Destekli HTTP protokolüne bakış.
    - Daha önceki sorunlara getirilen çözümler.
- SSL Sertifikaları.
- Kullanıcı doğrulama sistemleri.
- Nasıl bir SSL destekli HTTP sunucusu sahibi olunur.
- Bir gerçek yaşam örneği : “LKD SSL sunucusu”

HTTP Protokolü

HTTP protokolü, açık metin (clear text) olarak istemci ve sunucu arasında geçen bir mesaj trafiğidir.

Örnek bir mesaj HTTP oturumu

İstemcinin gönderdiği mesaj

```
| GET /~bdd/linux.php HTTP/1.1
```

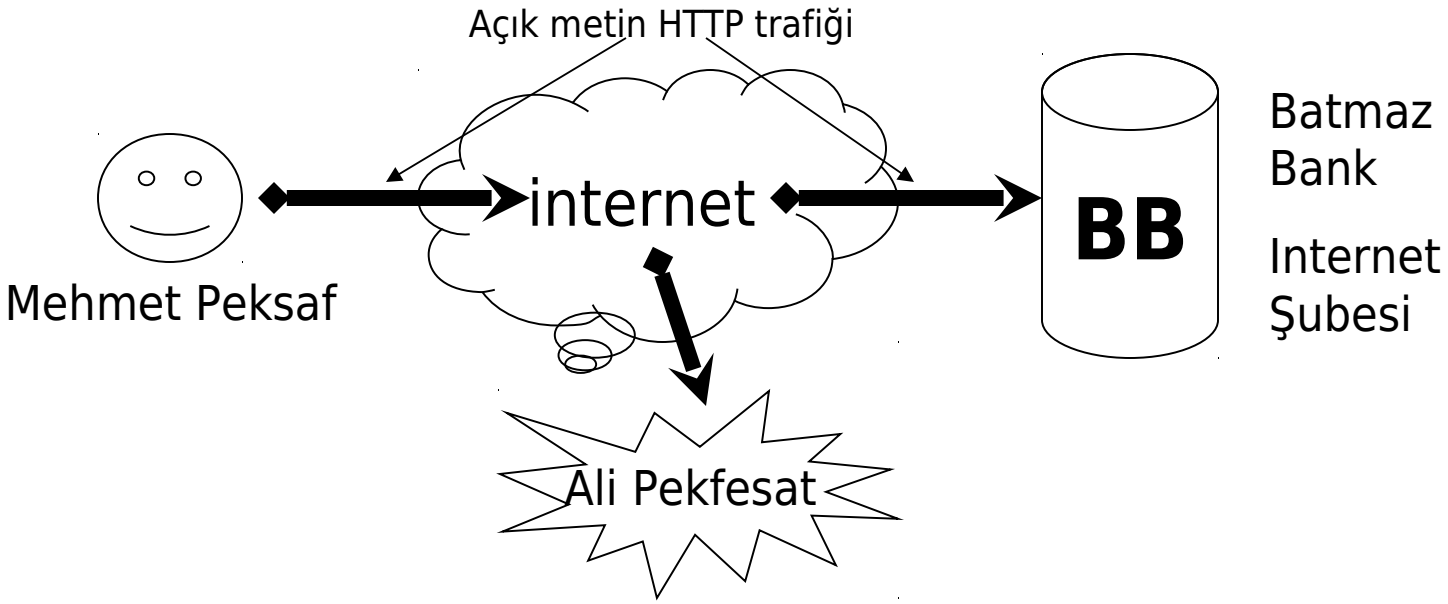
Sunucunun cevabı

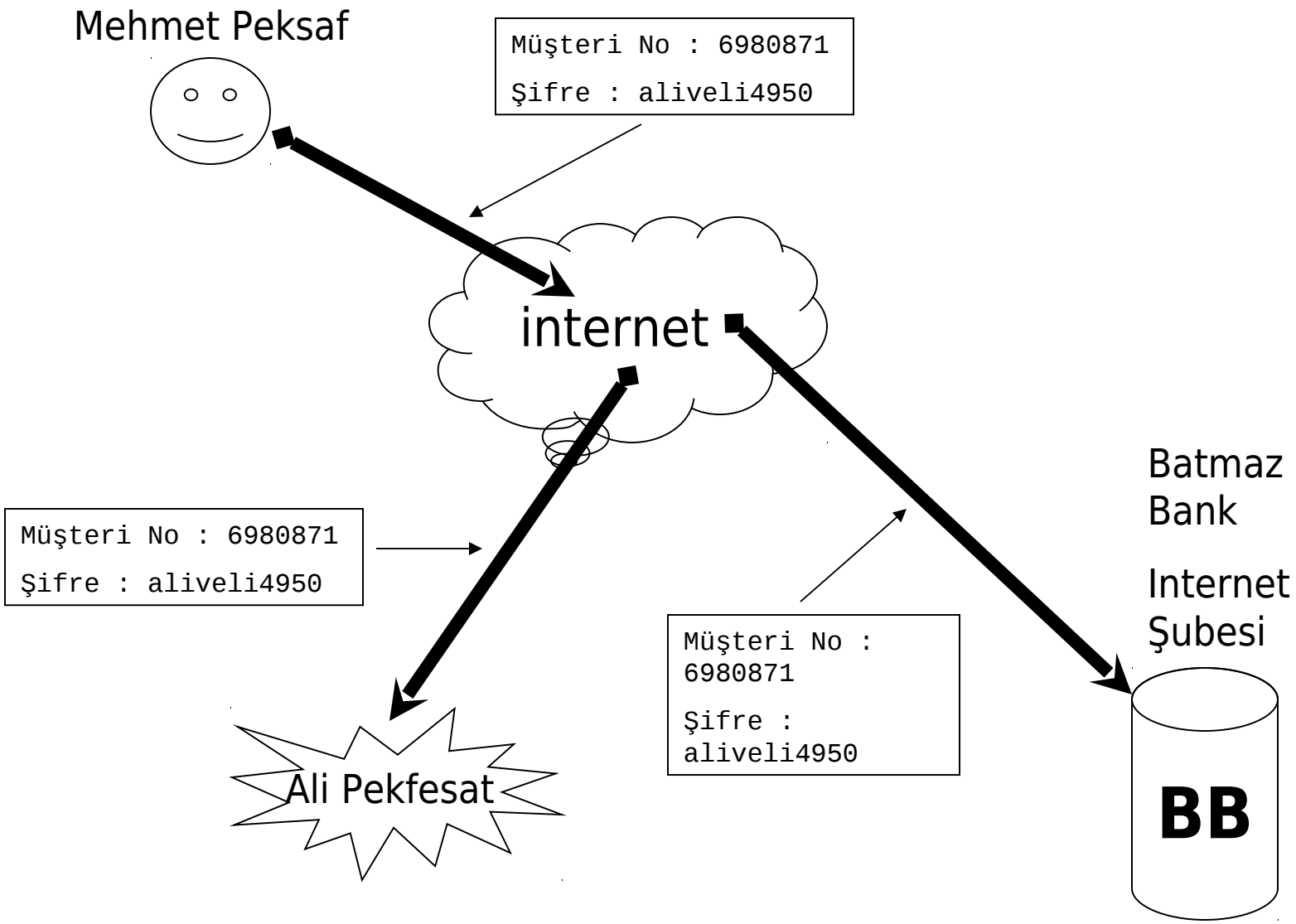
```
| HTTP/1.1 200 OK
| Date: Tue, 14 Nov 2000 16:43:10 GMT
| Server: Apache/1.3.12 (Unix)  (Red Hat/Linux) mod_ssl/2.6.4
OpenSSL/0.9.5a  PHP/4.0.1pl2
| Connection: close
| Content-Type: text/html; charset=iso-8859-1
| <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
| <HTML><HEAD>
| <TITLE>Welcome to Linux Pages</TITLE>
| </HEAD><BODY>
| <H1>Welcome to Linux Pages</H1>
| </BODY></HTML>
```

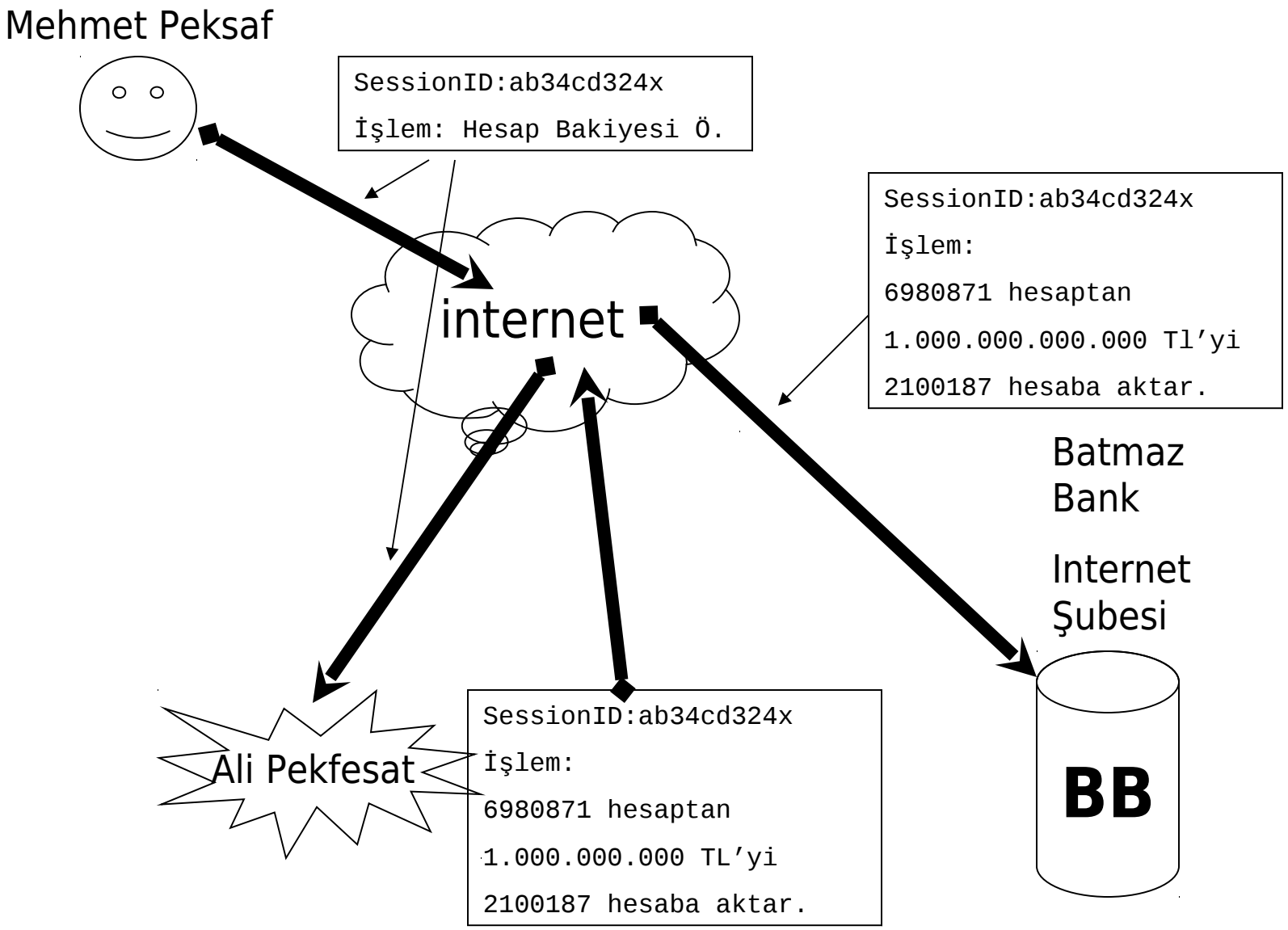
HTTP protokolü sebepli ortaya çıkan güvenlik açıkları.

• Açık metin akan Internet trafiği, kötü niyetli kişiler tarafından rahatlıkla dinlenebilir. *(Kişiye özel bilgilerin açığa çıkması)*

• İstemciden, sunucuya doğru giden bilginin yakalanıp, asıl bilgi yerine kötü niyetli kişiler tarafından giden bilginin gönderilmesi *(Görev kritik bilgilerin değişmesi, kişisel sistemlerin kötü niyetli yönetimi)*




Mehmet Peksaf
Müşteri No : 6980871
Şifre : aliveli4950
internet
Batmaz Bank
Internet Şubesi
Müşteri No : 6980871
Şifre : aliveli4950
Müşteri No : 6980871
Şifre : aliveli4950
Ali Pekfesat
BB


Mehmet Peksaf
SessionID:ab34cd324x
İşlem: Hesap Bakiyesi Ö.
internet
SessionID:ab34cd324x
İşlem:
6980871 hesaptan
1.000.000.000.000 Tl'yi
2100187 hesaba aktar.
Batmaz
Bank
Internet
Şubesi
BB
Ali Pekfesat
SessionID:ab34cd324x
İşlem:
6980871 hesaptan
1.000.000.000 TL'yi
2100187 hesaba aktar.

Çözüm Nedir ?

- Güvenli veri iletim kanalları
  - **extranet** (kiralık hat şeklinde)
  - **adanmış özel bağlantılar** (dial-up)

    (çok pahalı çözümler, son kullanıcıya hitap etmiyor)
- Şifreleme bazlı çözümler
  - **SSL** *(Ucuz !, Sadece istemci yazılımın desteklemesi yeterli)*
  - **IPSec** (en kesin, en modern çözüm; ancak yaygın değil)

    Layer 3 (ağ katmanı) 'de çalıştığı için IPSec Stack'i olan bir işletim sistemine duyulan ihtiyaç. IPSec trafiğini yönlendirme yetenekli yönlendiriciler (router))

SSL Protokolü

SSL protokolünün temeli kriptografi (şifreleme) olduğu için, kriptografik metotlar hakkında bilgiye ihtiyaç vardır.

Konvansiyonel Kriptografi :

“Simetrik kriptografi” olarak da bilinir. Mesajı şifreleyen, şifrelemede kullandığı gizli anahtarı, mesajın alıcısına bir şekilde ulaştırması gerekmekte. Alıcı ve gönderenden başkası gizli anahtarı bilmemelidir. Internet aracılığı ile gizli anahtarı ulaştırmak da güvenli değildir.

Açık Anahtar Kriptografisi :

“Asimetrik kriptograf” olarak da bilinir. İki ayrı anahtar kullanarak, gizli anahtar değişme problemine çözüm getirmektedir.

Bir kişinin iki adet anahtarı vardır. “Gizli Anahtar”, “Açık Anahtar”. Açık anahtar kullanılarak, herkes, sadece bu kişinin okuyabileceği şifreli mesajlar yaratabilir. Kişi, elinde gizli anahtarı bulundurduğu sürece, kendi açık anahtarını kullanılarak şifrelenmiş mesajları okuyabilir.

Kriptografik Teknikler (...devam)

Mesaj Özleri (Message Digest) :

Her ne kadar mesaj şifrelenmiş olsa da, bir başkası mesajın şifrelenmiş halini bozup, farklı bir hale getirebilir. Şifrelenmemiş mesajlarda ise, mesajın içeriği değiştirilebilir.

Mesajın güvenilirliğini kontrol etmek için, tek yollu öz fonksiyonları kullanılmaktadır. (MD5, SHA1, vs...)

Sayısal İmzalar :

Şifrelenmiş/Şifrelenmemiş mesajın kim tarafından gönderildiğini doğrulamak amacı ile sayısal imzalar kullanılır. Mesaj gönderen, anahtar ikilisinin (key-pair), gizli anahtarı ile, mesajı imzalar. Gönderen kişinin açık anahtarını bilmek, mesajın o kişiden gelip gelmediğini doğrulamak için yeterli olacaktır.

Kriptografik Teknikler (...devam)

Sertifikalar :

Her ne kadar şifreleme kullanılmış olsa da, bilgi gönderdiğiniz kişinin kim olduğundan emin olmanız gereklidir. Gönderdiğiniz bilgileri şifrelemek için kullanmış olduğunuz anahtarın, sertifikanın sahibine gerçekten ait olduğundan emin olmanız için gereklidir.

Bir sertifikaya güvenebilmeniz için, o sertifikanın daha önceden güvendiğiniz birisi tarafından imzalanmış olması gereklidir. (CA Certificate Authority)

Sertifika Otoriteleri (CA):

Bir sertifikanın içinde, sertifikanın ait olduğu kuruluşa ait bilgiler, açık anahtarı ve en önemlisi sertifikayı onaylayan kuruluşun sayısal imzası yer alır. CA, sayısal sertifikaları imzalayan üst otorite kurumuna verilen isimdir.

Kendi CA'nizi da oluşturabilirsiniz... Tüm SSL istemcileri tarafında güvenilen ticari CA kuruluşları: VeriSign, Thawte, GlobalSign, Entrust, DT, AT&T.

Bir SSL sunucuya nasıl sahip olunur ?

- **SSL** destekli bir HTTP sunucusunun kurulması.
- Anahtar çiftinin (açık/gizli anahtar) (key pair : public/private key)
- Sertifika İmzalama İsteği sertifikasının oluşturulması. (CSR)
- CA ile temasa geçme / Kendi CA'ni oluşturma.
- CA 'dan gelen, imzalanmış sunucu sertifikasının sunucuya yüklenmesi.

Bir SSL Sertifikasının görünümü:

Bir Netscape istemcisi ile, güvenli bölgenin detayları alınıyor.

LKD SSL sunucusunun sertifikası....

This Certificate belongs to:
www.linux.org.tr
webmaster@linux.org.tr
Bilgi Guvenligi Grubu
Linux Kullanicilari Dernegi
Ankara, TR, TR

This Certificate was issued by:
LKD Root Certificate Authority
bgg@linux.org.tr
Bilgi Guvenligi Grubu
Linux Kullanicilari Dernegi (LKD)
Ankara, TR

Serial Number: 01
This Certificate is valid from Tue Sep 12, 2000 to Wed Sep 12, 2001
Certificate Fingerprint:
BF:F1:06:75:DE:56:F4:77:82:C1:FD:34:A5:40:2B:62

LKD SSL Sunucusu :

- Listar, web ara yüzünün kurulması ile gelen, açık metin şifre trafiği sorunu...
- LKD ‘nin ileride vermeyi planladığı, kişisel gizliliğin ön planda bulunduğu projeler...

Nasıl Kuruldu ? :

- OpenSSL sisteme kuruldu.
- APXS desteğine sahip olan Apache sayesinde, Apache’yi yeniden derlemeye gerek kalmadan, “mod_ssl” de kuruldu.
- Apache + OpenSSL + mod_ssl RPM paketi olduğu için, sorunsuz ve zahmetsiz bir kurulum yaşandı.

Sorular :

- Apache nedir ?
- OpenSSL nedir ?
- mod_ssl nedir ?

LKD SSL Sunucusu : (devam ...)

- Kurulum ile birlikte gelen sertifika her ne kadar çalışan bir sertifika olsa da, sadece LKD'ye ait bir sertifika gerekliydi.
- LKD, Berk Demir tarafından CA ilan edildi, Selami Aksoy tarafından destek görüldü :-)
- LKD için CA sertifikaları oluşturuldu.

```
[root@ankara LKD_CA]# openssl genrsa -des3 -out ca.key 1024
[root@ankara LKD_CA]#  openssl req -new -x509 -days \
> 365 -key ca.key -out ca.crt
```

- LKD SSL sunucusu sertifikaları oluşturuldu.

```
[root@ankara]# openssl genrsa -des3 -out server.key 1024
[root@ankara]# openssl req -new -key server.key -out server.csr
```

DİKKAT ! : CommonName = FQDN

Örnek : CommonName : www.linux.org.tr

LKD SSL Sunucusu : (devam ...)

- CA haklarımızı kullanarak, www.linux.org.tr CN ‘li sertifika isteğini doğruladık ve sertifikayı imzaladık.

```
[root@ankara LKD_CA]# /usr/share/ssl/mod_ssl/sign.sh server.csr
```

- İmzalanmış sertifika sunucuya tanıtıldı.

```
[root@ankara LKD_CA]# cp server.key /etc/httpd/conf
```

```
SSLCertificateFile    conf/server.crt
SSLCertificateKeyFile conf/server.key
```

SONUÇ :

- Kişisel gizlilik gerektiren, görev kritik her türlü uygulamada, açık metin ile iletişim kuran sistemlerden uzak durulmalı.
- Ucuz ve kolay bir çözüm olan SSL ile kriptografik yaklaşım tercih edilmeli.
- SSL sadece HTTP amaçlı olarak kullanılmamaktadır. Bir çok VPN, Katman 7 (Layer 7/Uygulama Katmanı/Application Layer) uygulamalarını SSL tabanlı olarak çalıştırmaktadır.
- SSL her ne kadar, ucuz ve kolay bir güvenlik sistemi olsa da, ilerleyen yıllarda, IPSec'in yaygınlaşması ile etkinliğini yitirecektir.