Güvenli Kabuk: SSH

Burak DAYIOĞLU, Korhan GÜRLER
{bd,kg}@dikey8.com

İletişim Protokolleri ve Güvenlik

- Yaygın biçimde kullanılan pek çok iletişim protokolü, günün ihtiyaçları doğrultusunda, güvenlik gereksinimleri göz önünde bulundurulmadan geliştirilmiştir
  - Uzak erişim: Telnet/Rsh/Rlogin
  - E-posta: SMTP/IMAP/POP
  - Dosya iletimi: FTP/NFS
  - ...
- Bu protokoller, iletişimin güvenliği bağlamında
  - Gizliliği (kimse bizi dinlemesin/dinleyemesin)
  - Bütünlüğü (kimse gidip gelen mesajları değiştiremesin)

  sağlamaktan uzaktır

SSH nedir?

- Komut satırı uzak erişim protokolü ve bu protokol ile iletişim kuran yazılım seti
  - Telnet'in iletişim gizliliği ve bütünlüğü sağlayan bir biçimi
    - Uçtan uca şifreleme (*end to end encryption*)
    - Karşılıklı kimlik doğrulama (*mutual authentication*)
    - İletişim bütünlüğü (*communications integrity*)
- İletişim güvenliği gerektiren hemen her türlü uygulamada "güvenli tünel" olarak da kullanılabilir
  - Güvenli veritabanı bağlantısı, dosya transferi, …

SSH İletişiminin Gerçekleştirilmesi

- Sunucu üzerinde ssh sunucusu (`sshd`) çalıştırılır:
  - `service sshd start` (Red Hat Linux)
- İstemci bilgisayardan uzak sisteme bağlantı için ssh istemci programı uygun parametre(ler) ile başlatılır:
  - ssh senlik@penguen.linux.org.tr

SSH Sunucu Doğrulaması

- SSH istemcisi, bağlantı sırasında sunucunun kimliğini denetler
  - İstemci, doğru sunucuya bağlandığından emin olur

```
$ ssh root@penguen.linux.org.tr
The authenticity of host ‘penguen.linux.org.tr (192.168.1.1)' can't be established.
RSA key fingerprint is 2b:26:65:ae:4c:5e:5b:5a:00:a3:91:b8:24:75:16:88.
Are you sure you want to continue connecting (yes/no)?
```

  - Bağlantı gerçekleştirildiğinde sunucu anahtarı kaydedilir
- Her SSH sunucusunun bir anahtar ikilisi vardır
  - SSH, açık anahtarlı şifreleme üzerine kuruludur

SSH Sunucu Doğrulaması - 2

- SSH istemci ayarlarının tümü `~/.ssh` dizini altındadır
  - Sunucu ayarlarının tümü, `/etc/ssh` dizini altındadır
- İstemci tarafından doğruluğuna güvenilen tüm sunucu açık anahtarları `~/.ssh/known_hosts` dosyası içerisinde yer alır:

```
www.dikey8.com,144.122.171.171 ssh-rsa
  AAAAB3NzaC1yc2EAAAABIwAAAIEA0Yu6rY5zFb9/jVzsf4ZYsQt
  6RGetkgBu0NNlWTnVOf4TPVoNGVNf2DHEfHU=
penguen.linux.org.tr,192.168.1.1 ssh-rsa
  AAAAB3NzaC1yc2EAAAABIwAAAIEAvwSJTPGnMUjg0c1FNzxIcnE
  0z91TPHTLdT75wXOZPeoZN0+f90kj=
```

SSH Sunucu Doğrulaması - 3

- İdeal durumda, sunucu açık anahtarının çevrim-dışı güvenli bir biçimde istemci bilgisayarına yüklenmelidir
  - CD-ROM
  - Disket
  - ...
- Sunucu açık anahtarı `/etc/ssh/ssh_host_key.pub` dosyası içerisindedir
  - Sunucu açık anahtarının istemci üzerindeki known_hosts dosyasına uygun biçimde eklenmesi yeterlidir

SSH: Kullanıcı Doğrulama

- Geleneksel parola temelli kullanıcı doğrulama
  - Ön-tanımlı çalışma biçimi
- Açık anahtarlı doğrulama
  - Kullanıcı, kendisini tanımlamak için kullanacağı anahtar çiftini `ssh-keygen` programı ile üretir
  - Sunucu üzerinde “anahtar ile doğrulama” yöntemi ile giriş yapacağı hesaba açık anahtarını “güvenilen bir kullanıcı” olarak tanımlar
  - Kendi sistemi üzerinde yer alan gizli anahtar kullanıcının tanımlayıcısıdır
    - Gizli anahtar, çalınmaya karşı bir parola ile korunabilir

Kullanıcılar için Anahtar Üretimi

```
$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key
  (/home/bd/.ssh/id_dsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in
  /home/bd/.ssh/id_dsa.
Your public key has been saved in
  /home/bd/.ssh/id_dsa.pub.
The key fingerprint is:
47:c3:d1:48:45:85:04:34:0a:d1:2e:f2:2c:7b:96:7
  e bd@dikey8.com
```

Sunucuya Kullanıcı Anahtarı Yükleme

- Kullanıcı, açık anahtar doğrulaması ile bağlanmak istediği sunucu üzerinde `~/.ssh/authorized_keys` dosyasına anahtarının içeriğini (`id_dsa.pub` dosyası) eklemelidir:

```
ssh-dss AAAAB3NzaC1kc3MAAACBAMcNKokh49SBClZjQU+xx
  NMmo8TPWyAB9r2q/rpNY5sbaKFiTTa0cAcjqHvIBmovMamp79
  1H6DgC5jkhT8= burak@dikey8.com
```

SSH: `r*` Komutlarına Alternatifler

- SSH, geleneksel r* komutlarına güvenli bir alternatiftir; rsh, rcmd, rcp yerine ssh kullanılabilir
  - Uzaktan kabuk erişimi
    - **`ssh root@penguen.linux.org.tr`**
  - Uzaktan komut çalıştırma
    - **`ssh root@penguen.linux.org.tr date`**
  - Uzak sisteme dosya kopyalama
    - **`scp /etc/hosts root@penguen.linux.org.tr:/tmp/hosts`**

Sftp ile Güvenli Uzak Dosya Erişimi

- Ssh uygulamalarından birisi olan sftp ile sunucu üzerinde depolanan dosyalara güvenli erişim sağlanabilir:

```
sftp burak@www.dikey8.com
sftp> cd /tmp
sftp> put /etc/passwd
```

Zayıf Protokollere Destek

- Pek çok iletişim protokolünün güvenlik özellikleri yetersizdir
- Bu protokolleri güvenli hale getirmek iki biçimde mümkün olabilir
  - Tüm istemci ve sunucular değiştirilir
    - Pahalı, zahmetli, bazen mümkün bile değil
  - İlgili protokol, yüksek güvenliğe sahip bir diğer protokol üzerinden iletilir
    - İstemci ve sunucuların değiştirilmesi gerekmez
    - Masrafsız ve pratik
- SSH, tünellenmiş iletişim amacıyla da kullanılabilir

SSH ve Tüneller

- Port ilerletme (ing. port forwarding) özelliği ile tüneller
  - Yerel porta gelen verinin uzaktaki bir porta iletilmesi
  - İletişimin SSH tarafından uçtan uca korunması
    - Ucuz ve basit uçtan uca VPN uygulaması
- Avantajları
  - Karşılıklı kimlik denetimi
  - İletişim gizliliğinin ve bütünlüğünün sağlanması
  - Sıkıştırma ile, belli durumlarda, daha etkin bant genişliği kullanımı

DiKEY8

SSH Tünelleri: *Örnekler*

- IMAP E-Posta erişiminin tünellenmesi

```
$ ssh –L 5555:mail.dikey8.com:143
  burak@mail.dikey8.com
```

- GPRS üzerinden Telnet
  - Bant genişliği değerli; sıkıştırması anlamlı

```
$ ssh –C –L 23:www.dikey8.com:23
  korhan@www.dikey8.com

$ telnet 127.0.0.1
```

SSH Tünelleri: Diğer Örnekler

- X11, VNC ve diğer uzak masaüstü hizmetleri
- SMB
  - Windows ağları için yazıcı ve dosya paylaşımı
- NFS, AppleTalk
- POP, SMTP, NNTP
- HTTP
- Sistem olay kayıt sunucuları
  - Syslog
- Veritabanları
  - Oracle, DB2, MySQL, vb.

X Tünellemesi

- SSH sunucusu, ssh istemcisi ile gerçekleştirilen uzak kabuk erişimlerinde X tünellemesini otomatik olarak gerçekleştirir:

```
istemci$ ssh burak@www.dikey8.com
www$ xterm
```

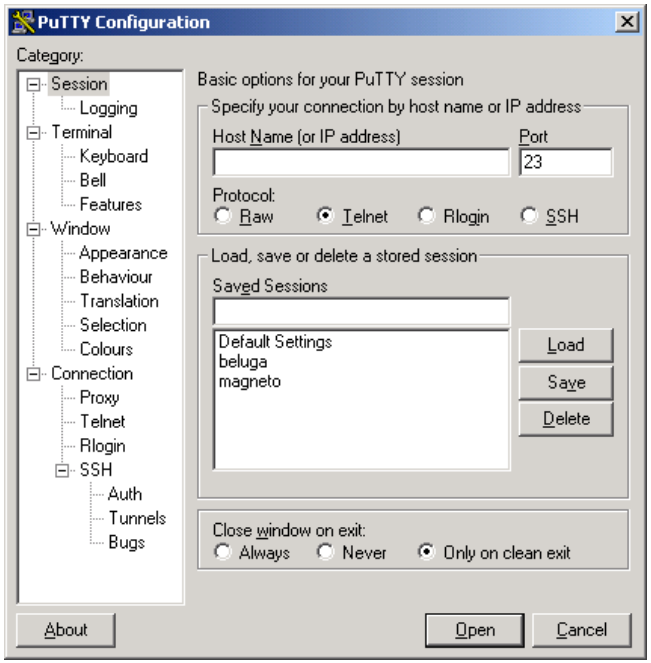
- `DISPLAY` değişkeninin belirlenmesi vb. gerekmez; X iletişimi ssh içerisinden tünellenir

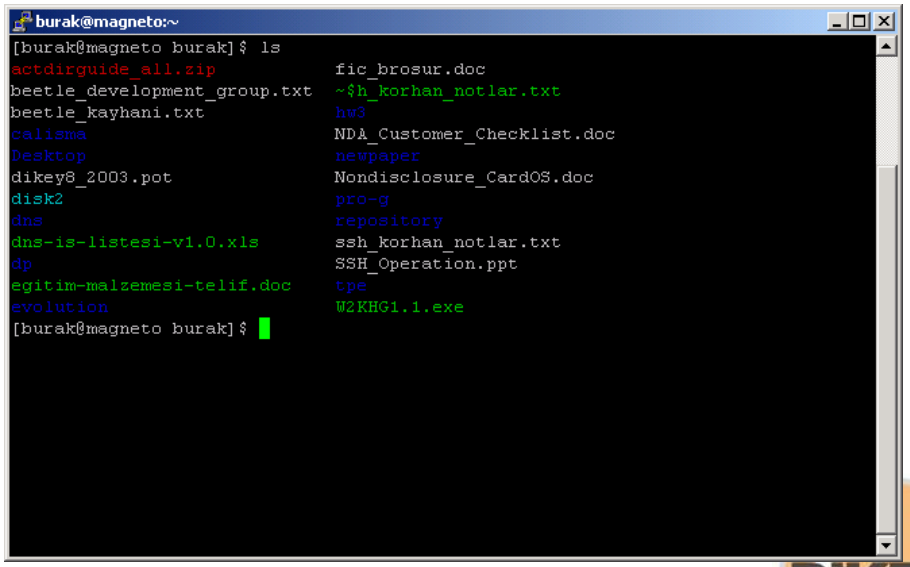
OpenSSH ve OpenSSL

- En yaygın özgür yazılım SSH kümesi OpenBSD ekibi tarafından geliştirilen OpenSSH paketidir
  - SSH sunucusu ve istemcisi
  - SFTP istemcisi ve sunucusu
  - Hemen tüm UNIX türevleri üzerinde çalışmaktadır
  - http://www.openssh.org
- OpenSSH, şifreleme kitaplığı olarak OpenSSL'i kullanmaktadır
  - Açık ve gizli anahtarlı şifreleme, mesaj özeti üretme, ...
  - OpenSSL tarafından desteklenen tüm hızlandırıcı kartlar OpenSSH tarafından da kullanılabilmektedir

Putty

- MS-Windows altında en yaygın istemcilerden birisidir
  - Özgür yazılım
  - ssh, scp, sftp ve diğerlerinden oluşan eksiksiz bir küme
  - http://www.chiark.greenend.org.uk/~sgtatham/putty/





Özet

- SSH paketi, güvenli iletişim için basit ve etkin bir altyapı sağlar
  - Güvenli uzak erişim
  - Güvenli dosya iletimi
- Açık anahtarlı kullanıcı doğrulaması parola korumasından daha etkindir; tercih edilmelidir
- SSH, zayıf protokollerin tünellenerek güçlendirilmesi için de kullanılabilir
  - TCP temelli hemen her protokol ssh içerisinden tünellenebilir