SSH Sunucusuna Nasıl Güveniyoruz?

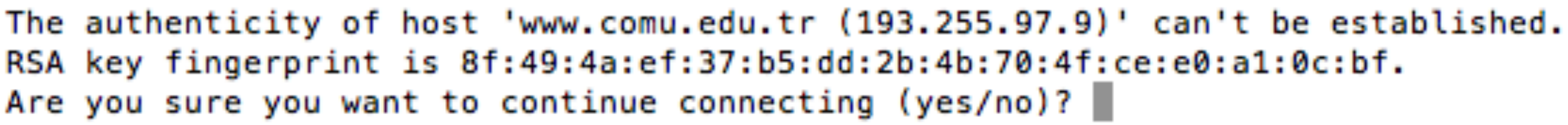
Necdet Yücel twitter.com/nyucel, TA3INC
Gülşah Köse twitter.com/gulsahkse, TA3IKG

ssh’ta problem mi var?

sunucu bizi kolay tanıyor

- kullanıcı adı / parola
- sertifika

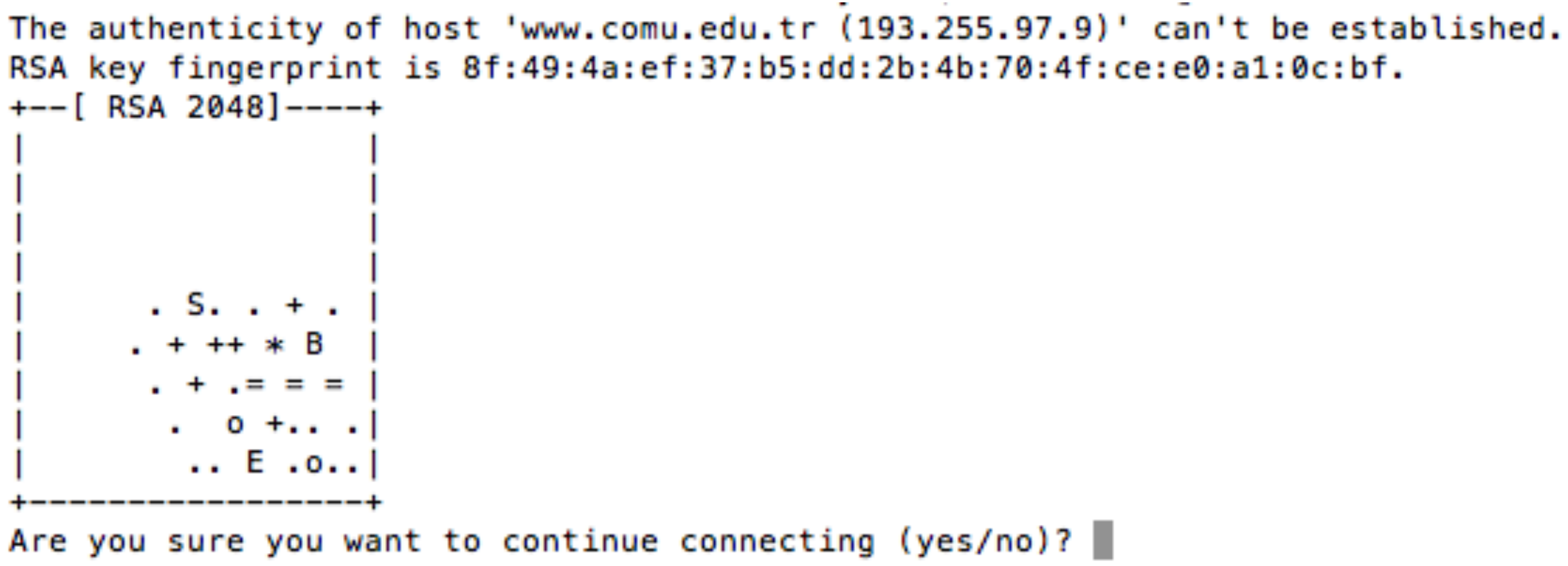
biz sunucuyu nasıl tanıyoruz?



```
The authenticity of host 'www.comu.edu.tr (193.255.97.9)' can't be established.
RSA key fingerprint is 8f:49:4a:ef:37:b5:dd:2b:4b:70:4f:ce:e0:a1:0c:bf.
Are you sure you want to continue connecting (yes/no)?
```

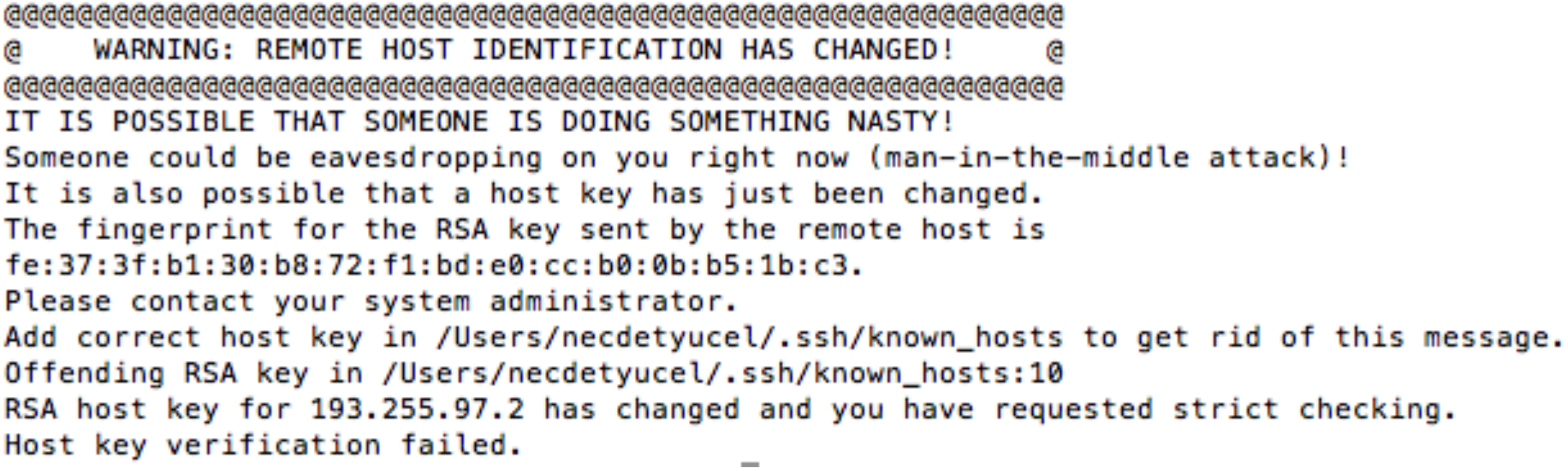
biz sunucuyu nasıl tanıyoruz?

`-o VisualHostKey=yes`



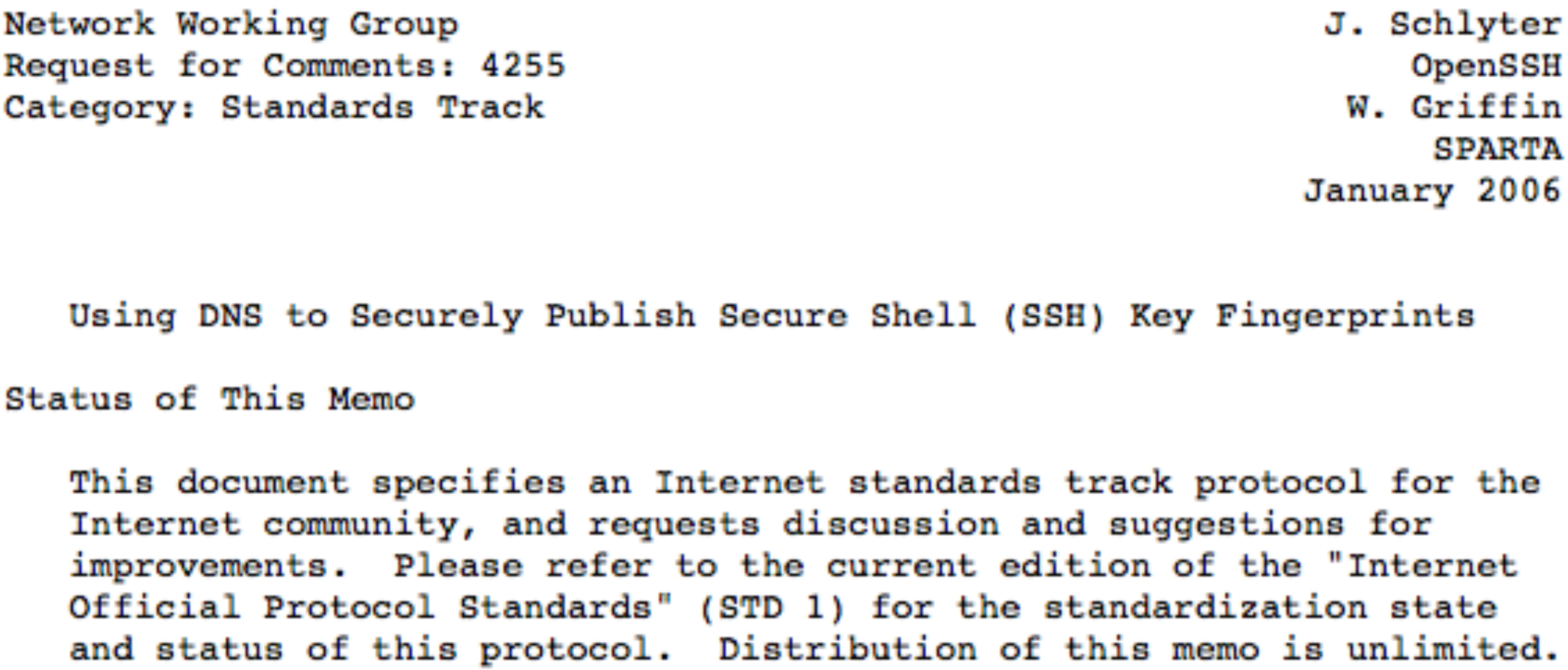
```
The authenticity of host 'www.comu.edu.tr (193.255.97.9)' can't be established.
RSA key fingerprint is 8f:49:4a:ef:37:b5:dd:2b:4b:70:4f:ce:e0:a1:0c:bf.
+--[ RSA 2048]----+
|                 |
|                 |
|                 |
|                 |
|      . S. . + . |
|     . + ++ * B  |
|      . + .= = = |
|       .  o +.. .|
|        .. E .o..|
+-----------------+
Are you sure you want to continue connecting (yes/no)?
```

Sunucu değişirse?



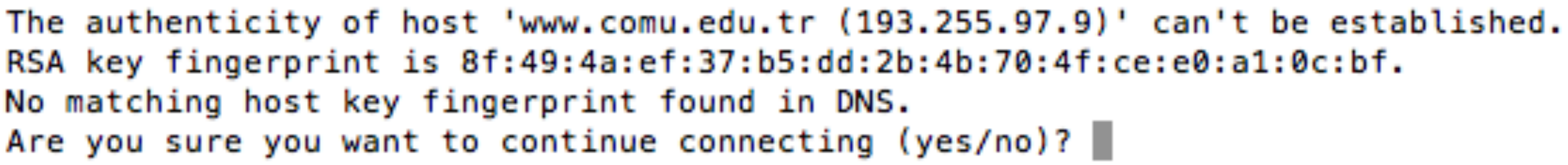
```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
fe:37:3f:b1:30:b8:72:f1:bd:e0:cc:b0:0b:b5:1b:c3.
Please contact your system administrator.
Add correct host key in /Users/necdetyucel/.ssh/known_hosts to get rid of this message.
Offending RSA key in /Users/necdetyucel/.ssh/known_hosts:10
RSA host key for 193.255.97.2 has changed and you have requested strict checking.
Host key verification failed.
```

DNS’e soralım http://www.rfc-editor.org/rfc/rfc4255.txt



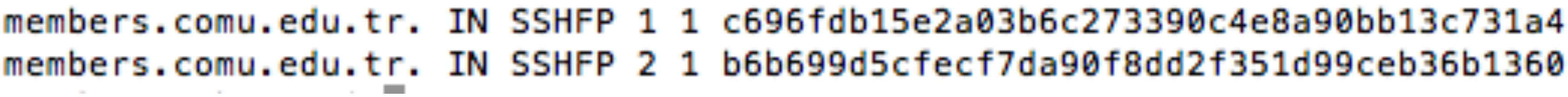
```
Network Working Group                                        J. Schlyter
Request for Comments: 4255                                       OpenSSH
Category: Standards Track                                     W. Griffin
                                                                  SPARTA
                                                            January 2006


   Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.
```

DNS’e soralım -o "VerifyHostKeyDNS=yes"

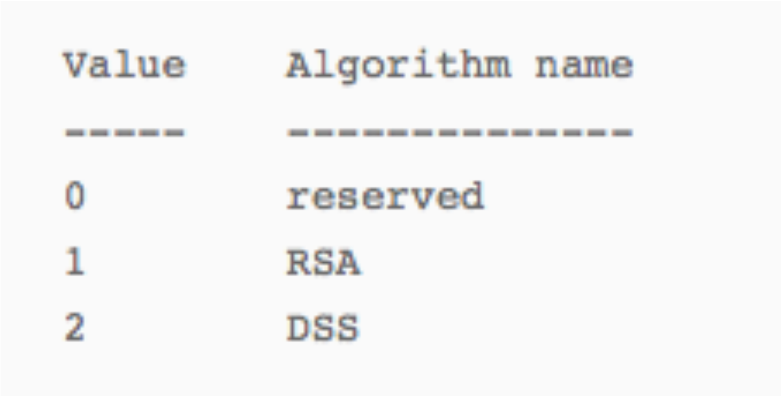


```
The authenticity of host 'www.comu.edu.tr (193.255.97.9)' can't be established.
RSA key fingerprint is 8f:49:4a:ef:37:b5:dd:2b:4b:70:4f:ce:e0:a1:0c:bf.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)?
```

DNS’e soralım ssh-keygen -r www.yourdomain.com.

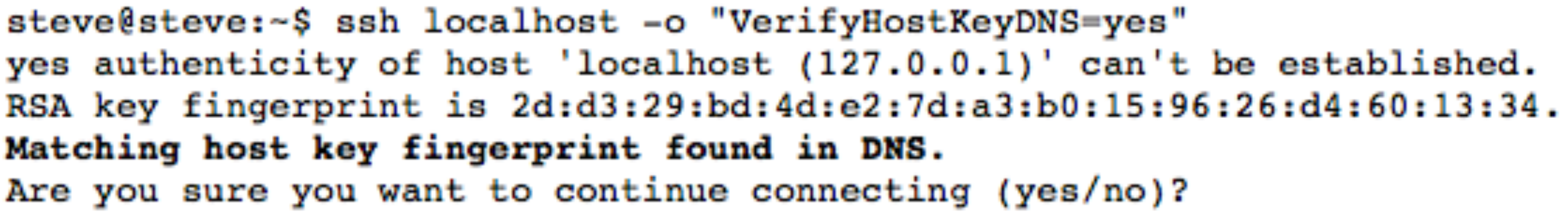


```
members.comu.edu.tr. IN SSHFP 1 1 c696fdb15e2a03b6c273390c4e8a90bb13c731a4
members.comu.edu.tr. IN SSHFP 2 1 b6b699d5cfecf7da90f8dd2f351d99ceb36b1360
```



```
Value     Algorithm name
-----     --------------
0         reserved
1         RSA
2         DSS
```

DNS’e soralım



```
steve@steve:~$ ssh localhost -o "VerifyHostKeyDNS=yes"
yes authenticity of host 'localhost (127.0.0.1)' can't be established.
RSA key fingerprint is 2d:d3:29:bd:4d:e2:7d:a3:b0:15:96:26:d4:60:13:34.
Matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)?
```

Teşekkürler