SSH Fingerprints

in the

Domain Name System

November 2006

Holger.Zuleger@hznet.de

The SSH Issue

- Who among you, has never seen this?

```
$ ssh zaphod
The authenticity of host 'zaphod.example.net (2001:db8:0:1::22)' can't be established.
RSA key fingerprint is 9c:70:35:27:4c:db:37:8f:42:b1:ba:4c:f0:90:50:a8.
Are you sure you want to continue connecting (yes/no)? _
```

- Who has ever press 'no' ?
- Who knows the fingerprint of an ssh server?
  - Who is the administrator of `zaphod`?
  - How to contact him?
  - In a secure way!
- SSH Fingerprints might be published
  e.g. on an HTTPS Server
- Ever heard about SSHFP ? (RFC4255)

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

SSH Fingerprints in DNS

- OpenSSH supports RFC4255 nearly since October 2003
  Was in draft status at this time (draft-ietf-secsh-dns-05.txt)

- Format of the SSHFP RR

```
hostname  IN  SSHFP algo fptype fingerprint
zaphod    IN  SSHFP 1    1      23D3C516AAF4C8E867D0A2968B2EB999B3168216
```

  algo: 1 == RSA; 2 == DSS
  fptype: 1 == SHA-1

- The Tool `ssh-keygen` is able to generate the DNS Record

```
$ ssh-keygen -r zaphod.example.net.
zaphod.example.net.  IN SSHFP 1 1 23D3C516AAF4C8E867D0A2968B2EB999B3168216
zaphod.example.net.  IN SSHFP 2 1 6C24ACBA790F7A666349AD49BC69C2D6A465E13A
```

- Yes, this is SSH version 2.0 only!
  But better to use SSH-2.0 anyway

SSHFP (Configuration)

- Escrow the SSH fingerprint in DNS
  - Add to Zonefile

    ```
    ssh-keygen -r `hostname` >> example.net.db
    ```

  - Increment serial number and reload zone

- Add the following to your client ssh config file:

```
Host zaphod
        HostName zaphod.example.net.
        VerifyHostKeyDNS yes  # or set to 'ask'
```

- Try again:

```
$ ssh zaphod
The authenticity of host 'zaphod.example.net (2001:db8:0:1::22)' can't be established.
RSA key fingerprint is 9c:70:35:27:4c:db:37:8f:42:b1:ba:4c:f0:90:50:a8.
Matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? _
```

- Ok, now you have to trust the DNS ...

SSHFP in secured DNS

- What about, if the DNS is secured
  (Remember, the AD bit has to be set in the answer)

```
$  dig +noall +comments +answer SSHFP zaphod.example.net
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63209
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 3

;; ANSWER SECTION:
zaphod.example.net.  10759  IN SSHFP  2 1 6C24ACBA790F7A666349AD49BC69C2D6A465E13A
zaphod.example.net.  10759  IN SSHFP  1 1 23D3C516AAF4C8E867D0A2968B2EB999B3168216
```

- A slightly more detailed output

```
$ ssh -v zaphod
OpenSSH_4.4p1, OpenSSL 0.9.8d 28 Sep 2006
debug1: Reading configuration data /home/hugo/.ssh/config
 ...
debug1: found 2 secure fingerprints in DNS
debug1: matching host key fingerprint found in DNS
debug1: ssh_rsa_verify: signature correct
 ...
Last login: Sun Nov 19 16:12:34 2006 from 1.2.3.4
zaphod:~$
```

Comments / Questions ?

Comments / Questions ?

http://www.hznet.de/dns/dns-sshfp.pdf

CONTENTS