

# Analysis of SSHFP records in the DNS

Sebastian Neef @ OARC-39

TU Berlin  
neef@tu-berlin.de

2022-10-23

# Agenda

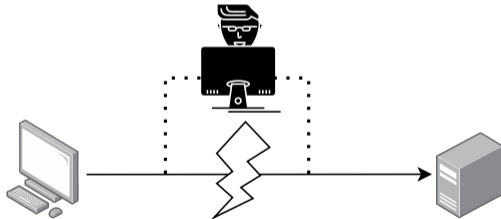
- 1 What is SSH host key verification?
- 2 What are SSHFP records?
- 3 What are our large-scale analysis results?

# Why do we need SSH host key verification?

- Establish the authenticity of the server we connect to.

```
[sneef@WorkTop ~]$ ssh -o VisualHostKey=no -o UserKnownHostsFile=/dev/null opendev.org
The authenticity of host 'opendev.org (38.108.68.124)' can't be established.
ED25519 key fingerprint is SHA256:vgW8X1bV3yT2jtmYZBLZ7o8uVhtvZq59dDNUVUYTRw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? 
```

- If not, malice-in-the-middle attacks are possible:



⇒ Login credentials or sessions could get compromised.

# How (not) to do SSH host key verification?

## Manual process

- 1 Ask the admin for the fingerprints
- 2 Manually compare both fingerprints
- 3 Continue or abort connecting

## DNS-based process

- 1 The admin publishes the fingerprints in the DNS (using DNSSEC!)
- 2 The openssh-client does the comparison
- 3 Continue or abort connecting

⇒ One method requires manual work and is error prone, the other requires a little more administrative work.

# SSHFP DNS records

- RFCs 4255, 6594, 7479, 8709 define how to store host key fingerprints in the DNS.
- Format: SSHFP <KEY-ALGO> <HASH-TYPE> <FINGERPRINT>

Table 1: Values for the SSHFP  
KEY-ALGO field.

Value	Algorithm	RFC
0	reserved	4255
1	RSA	4255
2	DSA	4255
3	ECDSA	6594
4	ED25519	7479
5	unassigned <a href="#">[1]</a>	-
6	ED448	8709

Table 2: Values for the SSHFP  
HASH-TYPE field.

Value	Algorithm	RFC
0	reserved	4255
1	SHA1	4255
2	SHA256	6594

# SSHFP DNS records

```
[sneef@WorkTop ~]$ dig SSHFP opendev.org +noall +answer +question
;opendev.org.                IN      SSHFP
opendev.org.                3600   IN      SSHFP   3 2 C9B288FF042ED0934FEB313BE277B546896C8C585FAED5C3057189A9 8585C5FD
opendev.org.                3600   IN      SSHFP   4 1 1D866A8F892294F28DB9E3CA7827FE8D4E93588E
opendev.org.                3600   IN      SSHFP   4 2 BE05BC5F56D5DF24F68ED9A661904B67BA3CB9586DBD9AB9F5D0CD51 55184D1C
opendev.org.                3600   IN      SSHFP   1 1 15D5F6642C9424BBE5DA0D8A99C0558B790A6C4D
opendev.org.                3600   IN      SSHFP   1 2 E9749FDE703418C5D810CEA7DDCF6639B2070CFA64020AC8F31B4671 FA6CAF01
opendev.org.                3600   IN      SSHFP   3 1 2E8E854928BE740BE49C754F99DEE256545338EE
```

```
[sneef@WorkTop ~]$ ssh-keyscan -D opendev.org
; opendev.org:22 SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
opendev.org IN SSHFP 1 1 15d5f6642c9424bbe5da0d8a99c0558b790a6c4d
opendev.org IN SSHFP 1 2 e9749fde703418c5d810cea7ddcf6639b2070cfa64020ac8f31b4671fa6caf01
; opendev.org:22 SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
opendev.org IN SSHFP 3 1 2e8e854928be740be49c754f99dee256545338ee
opendev.org IN SSHFP 3 2 c9b288ff042ed0934feb313be277b546896c8c585faed5c3057189a98585c5fd
```

# SSHFP DNS records

```
[sneef@WorkTop ~]$ dig SSHFP opendev.org +noall +answer +question
;opendev.org.                IN      SSHFP
opendev.org.                3600   IN      SSHFP   3 2 C9B288FF042ED0934FEB313BE277B546896C8C585FAED5C3057189A9 8585C5FD
opendev.org.                3600   IN      SSHFP   4 1 1D866A8F892294F28DB9E3CA7827FE8D4E93588E
opendev.org.                3600   IN      SSHFP   4 2 BE05BC5F56D5DF24F68ED9A661904B67BA3CB9586DBD9AB9F5D0CD51 55184D1C
opendev.org.                3600   IN      SSHFP   1 1 15D5F6642C9424BBE5DA0D8A99C0558B790A6C4D
opendev.org.                3600   IN      SSHFP   1 2 E9749FDE703418C5D810CEA7DDCF6639B2070CFA64020AC8F31B4671 FA6CAF01
opendev.org.                3600   IN      SSHFP   3 1 2E8E854928BE740BE49C754F99DEE256545338EE
```

```
[sneef@WorkTop ~]$ ssh-keyscan -D opendev.org
; opendev.org:22 SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
opendev.org IN SSHFP 1 1 15d5f6642c9424bbe5da0d8a99c0558b790a6c4d
opendev.org IN SSHFP 1 2 e9749fde703418c5d810cea7ddcf6639b2070cfa64020ac8f31b4671fa6caf01
; opendev.org:22 SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.7
opendev.org IN SSHFP 3 1 2e8e854928be740be49c754f99dee256545338ee
opendev.org IN SSHFP 3 2 c9b288ff042ed0934feb313be277b546896c8c585faed5c3057189a98585c5fd
```

```
[sneef@WorkTop ~]$ ssh -v -o UserKnownHostsFile=/dev/null -o VerifyHostKeyDNS=yes opendev.org 2>&1 | grep -P '(host.key)|(fingerprint)'
debug1: kex: host key algorithm: ssh-ed25519
debug1: Server host key: ssh-ed25519 SHA256:vgW8X1bV3yT2jtmMYZBLZ7o8uVhtvZq59dDNUVUYTRw
debug1: found 6 secure fingerprints in DNS
debug1: verify_host_key_dns: matched SSHFP type 4 fptype 2
debug1: verify_host_key_dns: matched SSHFP type 4 fptype 1
debug1: matching host key fingerprint found in DNS
```

## Tranco 1M

- 1M domains scanned
- 105 domains use SSHFP (0.011%)
- 75 servers run SSH
- 66 with  $\geq 1$  matching fingerprint
- 28 use DNSSEC



## Tranco 1M

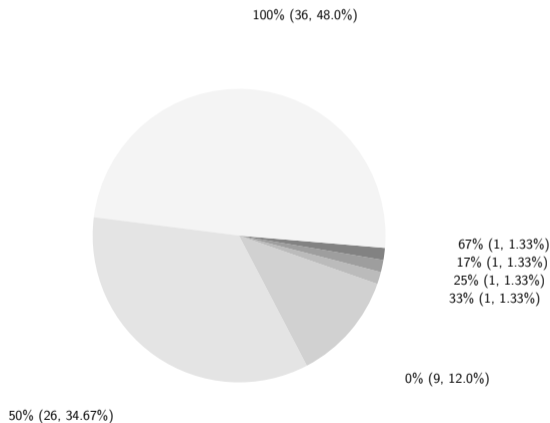
- 1M domains scanned
- 105 domains use SSHFP (0.011%)
- 75 servers run SSH
- 66 with  $\geq 1$  matching fingerprint
- 28 use DNSSEC

## Certificate Transparency Logs

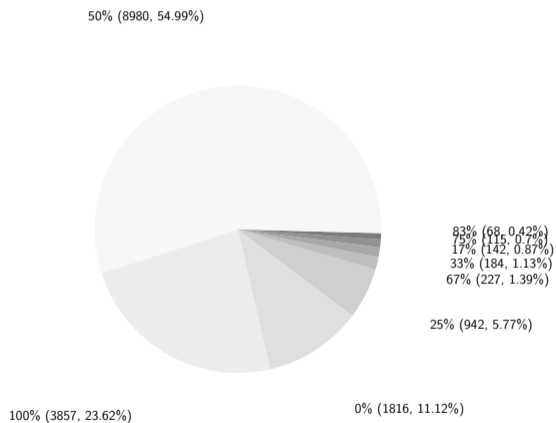
- 515M domains scanned (136M unique)
- 17,672 SSHFP sets (11,524 unique domains)
- 16,331 servers run SSH
- 14,515 with  $\geq 1$  matching fingerprint
- 3,896 unique domains use DNSSEC

# Large-scale analysis: Results (2)

- Less than 50% domains have 100% DNS-vs-server matching ratios

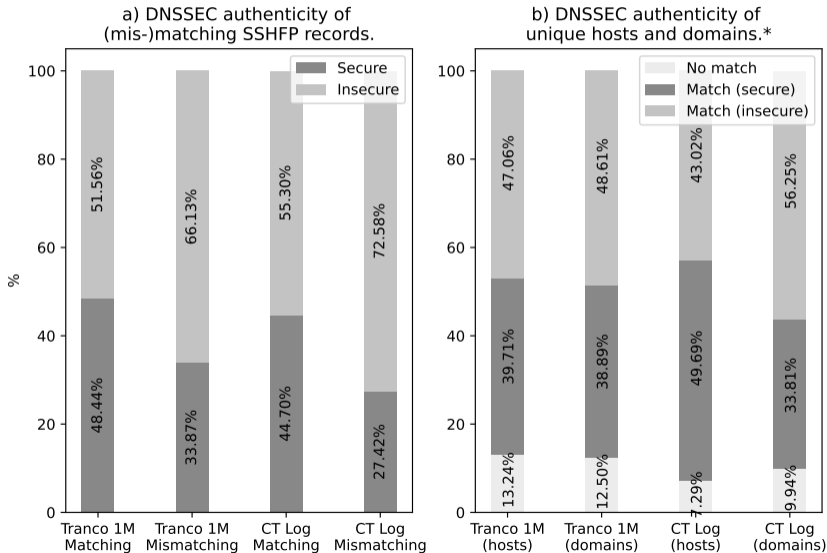


(a) Tranco 1M



(b) Certificate Transparency Log

# Large-scale analysis: Results (3)



# Conclusion

- Very few use SSHFP DNS records, although it is easy to setup.
- $\leq 50\%$  use DNSSEC, the rest misses out on security benefits.
- Try to make SSHFP records + DNSSEC more popular?

Thanks for listening!

# Questions?

Feel free to reach out: [neef@tu-berlin.de](mailto:neef@tu-berlin.de)

- 1 "Oh SSH-it, what's my fingerprint? A Large-Scale Analysis of SSH Host Key Fingerprint Verification Records in the DNS" - S. Neef, N. Wisiol
- 2 Repo with code & data - <https://github.com/gehaxelt/sshfp-dns-measurement>