DNSSEC / DANE demo

Paul Wouters
Senior software engineer,
Red Hat
October 17, 2015
Generating TLSA, SSHFP and OPENPGPKEY records

- `yum install hash-slinger`
- `tlsa --create www.example.com` (for https)
- `sshfp -a` (known_hosts)
- `sshfp -a -d -d nohats.ca -n ns0.nohats.ca` (axfr+scan)
- `openpgpkey --create pwouters@fedoraproject.org`
Verifying TLSA, SSHFP and OPENPGPKEY records

- `tlsa --verify www.example.com`
- `openpgpkey --verify pwouters@fedoraproject.org`
- `openpgpkey --fetch pwouters@fedoraproject.org`

```
[paul@bofh paul]$ tlsa -q -4 --create fedoraproject.org

No certificate specified on the commandline, attempting to retrieve it from the server fedoraproject.org. Attempting to get certificate from 152.19.134.146
Got a certificate with Subject: /serialNumber=eFvGaM1boCDI04Sq/5q3n25qNP78v3Ig/C=US/ST=North Carolina/L=Raleigh/O=Red Hat Inc/OU=Corporate Infrastructure Services/CN=*.fedoraproject.org
._443._tcp.fedoraproject.org. IN TLSA 3 0 1 8f0f2374f2fdb57ef0ddcc2704a1519ba7757aed34145dc8a83236b5c16af0db
```
Configure postfix to use TLS

- Generate TLS key, certificate and CA-certificate
- Enable TLS in postfix:
  - `postconf -e "smtpd_tls_security_level = may"
  - `postconf -e "smtpd_tls_key_file = /etc/postfix/ssl/server.key"
  - `postconf -e "smtpd_tls_cert_file = /etc/postfix/ssl/server.pem"
  - `postconf -e “smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem”
  - `postconf -e "smtpd_tls_security_level = may"
  - `postfix reload"
Configure postfix to use DNSSEC and DANE

- `postconf -e "smtp_dns_support_level = dnssec"`
- `postconf -e "smtp_tls_security_level = dane"`

- Ensure the server postfix runs on is configured to use a DNSSEC capable server specified in `/etc/resolv.conf` (you can point to 8.8.8.8 or 193.110.157.123)
Postfix now requires TLS when a TLSA record is present

```
[root@mx etc]# tail -f /var/log/maillog
Oct 17 22:05:28 mx postfix/smtpd[28105]: NOQUEUE: reject: RCPT from whisk.cs.uwaterloo.ca[198.96.155.11] ineto=<<dlm@upzeqbep.com.tw> to=<cypherpunks@nohats.ca> proto=ESMTP helo=<mail.paip.net>
Oct 17 22:06:39 mx postfix/pickup[27540]: 3ndb336nTzzChB: uid=0 from=<root>
Oct 17 22:06:39 mx postfix/cleanup[28304]: 3ndb336nTzzChB: message-id=<3ndb336nTzzChB@mx.nohats.ca>
Oct 17 22:06:40 mx opendkim[11693]: 3ndb336nTzzChB: no signing table match for 'root@mx.nohats.ca'
Oct 17 22:06:40 mx opendkim[11693]: 3ndb336nTzzChB: no signature data
Oct 17 22:06:40 mx postfix/qmgr[27541]: 3ndb336nTzzChB: from=<root@mx.nohats.ca>, size=448, nrcpt=1 (queue: 28310)
Oct 17 22:06:41 mx postfix/smtp[28310]: 3ndb336nTzzChB: to=<paul@bofh.nohats.ca>, orig_to=<paul@bofh.nohats.ca>, dsn=4.7.4, status=deferred (TLS is required, but was not offered by host bofh.nohats.ca)
```

Paul Wouters <pwouters@redhat.com>
Postfix validates the TLSA record before sending email

```
[root@mx etc]# tail -f /var/log/maillog
Oct 17 22:22:50 mx postfix/pickup[28750]: 3ndbPk5GY3zChB: uid=0 from=<root>
Oct 17 22:22:50 mx postfix/cleanup[28756]: 3ndbPk5GY3zChB: message-id=<3ndbPk5GY3zChB@mx.mxe.net> <3ndbPk5GY3zChB@mx.mxe.net>
Oct 17 22:22:50 mx opendkim[11693]: 3ndbPk5GY3zChB: no signing table match for 'root@mx.mxe.net'
Oct 17 22:22:50 mx opendkim[11693]: 3ndbPk5GY3zChB: no signature data
Oct 17 22:22:50 mx postfix/qmgr[28751]: 3ndbPk5GY3zChB: from=<root@mx.nohats.ca>, size=47023, nrcpt=1 (queueing)
Oct 17 22:22:51 mx postfix/smtp[28763]: 3ndbPk5GY3zChB: to=<paul@bofh.nohats.ca>, relay=bofh.nohats.ca.in-addr.arpa [192.0.2.180]:58716 (200.0.0.1) at Thu, 18 Sep 2020 00:22:51 -0700
Oct 17 22:22:51 mx postfix/qmgr[28751]: 3ndbPk5GY3zChB: removed
```

Publishing an OPENPGPKEY:

- Generate a new gpg key, for example using gnupg

```
[demo@thinkpad ~]$ ls -a
  .  .bash_logout .bash_profile .bashrc .lesshst .mozilla .xauthKRKwel
[demo@thinkpad ~]$ gpg --gen-key
gpg (GnuPG) 1.4.19; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory `~/home/demo/.gnupg' created

gpg: new configuration file `~/home/demo/.gnupg/gpg.conf' created

gpg: WARNING: options in `~/home/demo/.gnupg/gpg.conf' are not yet active during

gpg: keyring `~/home/demo/.gnupg/secring.gpg' created

gpg: keyring `~/home/demo/.gnupg/pubring.gpg' created

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0) 60
Key expires at Wed 16 Dec 2015 03:25:27 PM EST
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
```
Publishing an OPENPGPKEY:

- Generate a new gpg key, for example using gnupg

Real name: Demo User
Email address: demo@nohats.ca
Comment: Demo User
You selected this USER-ID:
  "Demo User (Demo User) <demo@nohats.ca>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? 0
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
........+++++
........+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
........+++++
................+++++
gpg: /home/demo/.gnupg/trustdb.gpg: trustdb created
gpg: key B9346B91 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2015-12-16
pub 2048R/B9346B91 2015-10-17 [expires: 2015-12-16]
  Key fingerprint = 7524 CABB 911E 7899 B987 4725 B541 B908 B934 6B91
uid Demo User (Demo User) <demo@nohats.ca>
sub 2048R/A8BE9C30 2015-10-17 [expires: 2015-12-16]
Publishing an OPENPGPKEY:

- Create an OPENPGPKEY record (in generic format)
Publishing an OPENPGPKEY:

- Create an OPENPGPKEY record (in rfc format)

```
[demo@thinkpad ~]$ openpgpkey --create demo@nohats.ca --output rfc
```

```
[demo@thinkpad ~]$ openpgpkey --create demo@nohats.ca --output rfc
```

```
8b1c1c1ea6c650485e77efbc336c5bfb84ffe0b0bea65610b721762._openpgpkey.nohats.ca. IN OPENPGPKEY mQ
M4Tdg7gMkgs4AwMH1LWTTLFdHt9NKBp5ZNmc+Fx1/Ny0NRQdJa2GSX1IYgwPFfRo4NZM1qh43cGAaXYzANYvng12nheN/Jk0
00sxEAXEzE5Ahio1vUv+warpILts0nBHEWcW90e6F0XPeKt4Nxl2LMQHHV5heyVIv8GBfzlTCBnpYV2878G/x5iO3Ec/jjKN
IzdpBVkhrTRPzASZRl8ceH19XygSwWlh4rMjB/SlgkGk8qL7ABEBAAg0JkrLbW8gVXNliAoRGVtbyBvc2VykKSA8ZGVTb0Bub2h
oABgsJCAcDAgYVCAIJCGsEFgIDAQIeAQIXgAAKCRC1qbk1uTRkXoJB/9tOB9He9kBPMQmBNU2z0cgZv0ZKMLXkMQp4HTesB
iry320AVgmBU06M72AwoeotjBU2x7d1LwJj1PszhVdfHTTMz25BGsZNDQqUGWcSmOxiJo/Ps00jy5hGDEFiyxtX11v+M4X
r/oxxbrMUKnESZtp14c9X+xowYP016un9K8H0JVU1LRvczaA0yRLNe+SMQccCpe6Z8Y7/UAnEmG6YQlxpwK0EHz+Sw2iyRkz4
irugBCADbMY4vI+f7WdZQKG/CJxV0aguTuaJ6Gq/VHFHaKsuDTDgBDG5H6GF5mO+AqIJdwcGJpbnTi3LX2FwWDVfpiN8va/
1NWxYtxHqHsIp0n6BeBrKS2JyvnNciIiIsgp5s8awxj+zumjloZyujhm5dycpubeOLkyDyRPB3yf xl7oKNzePqS0tQ49CPu3UHh+
svuxMzX8/+sYziQ8aRmQUTExrK4Us6aazrkpwez4DZNSb2s5K2dN/dtHr78fMzzJRaeahKDVhajJrobABEBAAgJASUEGeACa
Hwf+OAH/V0yosszIhD0cymporj+zKwhHCNLMqMvKpn6UxcAdmaq0Ul/eKrmt20ReyMQ7Dik1LLCg61Ebq05iULi4qkuqYt7mm
cccc+kG7wvsBuzgAhRgCe5QsASezzvs3cQ4v5EnaGExUBF1mIDMUM3URfgNo1DIhgyLgkZZnXwI9/5SUE0490JRn/3KZM1v6j
P1Q2YCKp0qOLxv2IoteEf0vyXILHPZodsc/mxoPp0sUCZuqBjOtdB11ArRf8x9ucu5EPhc2qflg==
```

[demo@thinkpad ~]$
Publish your OPENPGPKEY and verify it:

- Add record to zone, re-sign and propagate zone, then:

```bash
$ openpgpkey --fetch demo@nohats.ca

BEGIN PGP PUBLIC KEY BLOCK
Comment: demo@nohats.ca key obtained from DNS
Comment: key transfer was protected by DNSSEC
Version: GnuPG v1
mQENBFYirugBCADqhlNam3SgQnEYWCSnygmHheZQM4Tdg7gMkgs4AwMH1LWTTLF
dHt9NKBp5ZNnC+Fx1/Ny0NRQdJa2GSX1lYgwPFRYo4NZM1qh43cGAaXYzANYvngi
azrkpwez4DZNBSb2s5K2dN/dtHr78fMzzJrAeahKDVhaJrobABEBAAGJASUEGAEC
AA8FAlYirugCGwwFCQBPGgAACgkQtUG5CLk0a5HBHwf+0AH/V0y0sszIhD0cymop
Rj+zKwhHCNLqMv kpN6Ux Admaq0Ul/eKRmt20ReyMQ7Di kLCgL61E bgQ5iULi4q
kuqYt7mmTwP Ml0qSY6zk/ZM4DEyx+0Kc Ty0B vsHDX02 kcknc++kG7w sBU zgz AhR
gCe5QsASezzvs3cQ4v5EnaGE XuBF1mIDMU3URf gNo1DIhg wyLGkZZnX wI9/5SUE0
490JRn/3KZM1v6jLfBvNEIeXR NrphjB8/rtxUZoCMsKow32pFRRdcF0P1Q2YCKp0q
0LX v2ioteEf0vyXILHPZodsC/mxoPp0sUCZ uQbJ Y0dTb11ArRf8X9uc u5EP hC 2q f
lg=
=LGuo
END PGP PUBLIC KEY BLOCK
```
openpgpkey tool warns about email mismatch

[Demo@thinkpad ~]$ openpgpkey --fetch paul@bofh.nohats.ca
openpgpkey: Received OpenPGP data does not contain a key with keyid paul@bofh.nohats.ca
(add --uid <uid> to override with any of the below received uids)
# Paul Wouters (migration only, use new key) <paul@bofh.nohats.ca>
# Paul Wouters <paul@xtdnet.nl>
# Paul Wouters <paul@freeswan.nl>
# Paul Wouters <paul@freeswan.org>
# Paul Wouters <paul@xelerance.com>
# Paul Wouters <paul@cypherpunks.ca>
# Paul Wouters (migration only, use new key) <paul@bofh.nohats.ca>
[Demo@thinkpad ~]$ openpgpkey --fetch paul@bofh.nohats.ca --uid paul@bofh.nohats.ca | head -15
------BEGIN PGP PUBLIC KEY BLOCK------
Comment: paul@bofh.nohats.ca key obtained from DNS
Comment: key transfer was protected by DNSSEC
Version: GnuPG v1

mQENAz97DD0AAAEH/2hrtp4YrNMc0AAF8YbM8ryWi8uH/dTFzV2pLMt+CVh7V5EGN7icm8n+aXU3eY+pvftjixj0kvEJmc01lfbvG+4Bus4cn2NtM7Yy0kZLSE050bkno
OE+WX9/ffbnoXQcnk/E6DBn0sIaxPCxnlM25V6UtGKnkeC3t0CUCwfrMtQaqkUhhqN
gfDip45HlrbPGnr4EX+Ck52HPe7/neO9w4SXR4pWNQ50c1JXfBpwZVPedx9f0ys
ARBH6uk4BQbxDGVBj5S2n2oopnZ4L+GvDW7ltcfZlJmaCoZUoH9eWMWX35fJ4phra
aK3C3INDF8pquC+66kLEabffyEHW5xgprXMj+EABRG0HVBhdMwgV291dGVycyA8
cGF1bEB4dGRuZXQubmv+iQEVAwU4TP3tGiuCyBqi1zCfhAQHBofwQd57/Ag1Sf4S
J1w9wyzm4KxeQs8s38s318FDvrdXiXlHbGdUz6ErFIMMKt5wYag2lrBjP4t06fg4H6
90Pj+hSjN6DLnVtJRGYYASC53m9DTYbnN1KVBBr/VmyrCtgzEhZmNlLlxLx0PB
Ut04+K9z1/SIFqcfmBe61ZQ2yZ7zADD+K7w7b0x8tfr0BXZSRpDpi/RBATmjFDZ
Demo of openpgpkey-milter using OPENPGPKEY

[root@mx ~]# jobs
[1]+ Running tail -f /var/log/messages &
[root@mx ~]# mail paul@bofh.nohats.ca
Subject: test icann
testing icann demo
.
EOT
[root@mx ~]# 0 Oct 17 22:52:14 mx openpgpkey-milter: connect from localhost at ('127.0.0.1', 0)
Oct 17 22:52:14 mx openpgpkey-milter: Received DNSSEC secured OPENPGPKEY for paul@bofh.nohats.ca:
Key-ID:E71806A6B5CC27E1 Fingerprint:FC0C977F4724D0EA06E31C2AE3BA29CE
Oct 17 22:52:14 mx openpgpkey-milter: Will encrypt message to fingerprints:FC0C977F4724D0EA06E31C2AE3BA29CE
View of email send via postfix + openpgpkey-milter

Date: Sat, 17 Oct 2015 16:52:14
From: root <root@mx.nohats.ca>
To: paul@bofh.nohats.ca
Subject: [openpgpkey-milter encrypted message]

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.14 (GNU/Linux)

hQEMA+cYBqalzcFhAQf/WBtaZjQsc7EKIEtwhy7ox5tr10izCIsXCGvmbiV1Q+M1mZIKVF8ldAGV5Uo5PMuU1grTa0tawITy5C50CYgEFcFgFCy8LRt0LPoT50WkdBo0dfQbCbyBuB3RFeZHGAvxRroUSHI99EZDq72Hza/faUVJKFof0C1cBCYM6er7ImyYAg6Ua7YXouR7gL1MchsfDF48MWhJeapnMfl7lP7C+wGPO3xefzrBVt5G47rWwXDDvnN5Qs/1tFTHwEe6r1Ut9txT1eYEN1NZV8V1VucvBa7Fq61Cg73GAWcBGwnED8L9V1+RcpgQnZs7mLo1w0ppp3ZT3gwL2TuNa0bZqoy+cPa8nAXfBiRoa/JcQRBrQR+mCyhq+rzyUu+FUFqVnEcCcv19AR3UDcW0T+rxfxMuPGfITExVxs8+mJb50wqRLnpsNuqRwpx3FgyG3ItqRBC+211QwnzjKsgSp70YHB2ox7rby+t60756MxGhiP3gfNIjPTuCDfT9B0TNaxXD0WkzquY0rQ7lk78tiv+svFdmUpgAT6ovJ1lxkftZ5ZIVhwqYgcMqdzp0Y+lpJeBuJK9M4g6Ib0W6n/itLAl8tw2X8Wz7WrcYGKsKOSlyPxNaulQtzOqKqmWdgqHSeWEN2l0WS/xYRxK7qqLffnn8rZx4EUKeCZXbsegAWo/TYY7c1qW791qHqHlsL2mIN0w1b6TyYogwq56q99lwR1kQviA==
==fFWC
-----END PGP MESSAGE-----

[ALL of message]
SSHFP record: enable DNSSEC in ssh client

- Can be done in user's own ~/.ssh/ssh_config
- Can be done globally in /etc/ssh/ssh_config

- To only display extra informational text for ssh, use:
  
  VerifyHostKeyDNS ask

- To automatically accept the key when found in DNS
  
  VerifyHostKeyDNS yes
Connecting with ssh using VerifyHostKeyDNS ask

```bash
[root@ns0 ~]# dig +dnssec sshfp bofh.nohats.ca

;; DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 +dnssec sshfp bofh.nohats.ca
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 64517
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bofh.nohats.ca. IN SSHFP

;; ANSWER SECTION:
bofh.nohats.ca. 3600 IN SSHFP 1 1 C5B3A4D944A2973F3FEBFFB6592E34E295C44F798
bofh.nohats.ca. 3600 IN SSHFP 2 1 41E9A94810955E22CB437704D8F7F7DED08ECFAF

;; AUTHORITY SECTION:
nohats.ca. 86393 IN NS ns0.nohats.ca.
nohats.ca. 86393 IN NS ns1.nohats.ca.
nohats.ca. 86393 IN NS ns2.foobar.fi.
```

[root@ns0 ~]# ssh root@bofh.nohats.ca
The authenticity of host 'bofh.nohats.ca (76.10.157.69)' can't be established.
Matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? [y/n]
Connecting with ssh using VerifyHostKeyDNS yes

tail -10 /etc/ssh/ssh_config
# ForwardX11Trusted yes
# Send locale-related environment variables
SendEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
SendEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
SendEnv LC_IDENTIFICATION LC_ALL LANGUAGE
SendEnv XMODIFIERS

VerifyHostKeyDNS ask
VerifyHostKeyDNS yes

grep bofh .ssh/authorized_keys

ssh root@bofh.nohats.ca
root@bofh.nohats.ca's password:
ssh client detecting Man-in-the-middle attack

```
[root@ns0 ~]# dig sshfp rogue.nohats.ca.
; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> sshfp rogue.nohats.ca.
; global options: +cmd
; Got answer:
; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 61386
; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

; QUESTION SECTION:
rogue.nohats.ca. IN SSHFP

; ANSWER SECTION:
rogue.nohats.ca. 3575 IN SSHFP 1 1 00000000000000000000000000000000000000000000000000000000000000000000000000000000
rogue.nohats.ca. 3575 IN SSHFP 2 1 00000000000000000000000000000000000000000000000000000000000000000000000000000000

; Query time: 0 msec
; SERVER: 193.110.157.123#53(193.110.157.123)
; WHEN: Sat Oct 17 15:59:57 2015
; MSG SIZE  rcvd: 101

[root@ns0 ~]# ssh rogue.nohats.ca.
@  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 the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
Please contact your system administrator.
Update the SSHFP RR in DNS with the new host key to get rid of this message.
The authenticity of host 'rogue.nohats.ca. (193.110.157.104)' can't be established.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)?
```