Opportunistic Encryption revisited

(We're getting the cypherpunks band back together)

Paul Wouters
pwouters@redhat.com

Nov 7, 2013

Terminology was discussed yesterday at perpass

- Opportunistic Encryption means many different things
- I use the old FreeS/WAN definition
- Encrypt between two endpoints without specific setup
- Can be "anonymous" (no authentication)

draft-wouters-dane-openpgp-01

Publish OpenPGP key in DNSSEC to allow mail clients, MUA and MTA's to encrypt on the file.

```
echo "‘python -c ’import base64; print base64.b32encode("paul")’‘" \
  "._openpgpkey.nohats.ca IN TYPE65280 \\# \
  (" ‘gpg --export --export-options export-minimal \
  paul@nohats.ca | base64 | wc -c‘ ; gpg --export \
  --export-options export-minimal paul@nohats.ca | \
  base64; echo ")"

 dig +dnssec -t TYPE65280 obqxk3a=.\_openpgpkey.nohats.ca
```

TODO: Write postfix/sendmail milter proof of concept

draft-wouters-edns-tcp-chain-query and draft-wouters-edns-tcp-keepalive

Both drafts are meant to speed up DNSSEC on high latency links (read: phone)

- Improve client - server communication to keep TCP 53 open
- Get all DNSSEC data for validation of IPSECKEY record in one round trip

old FreeS/WAN OE

1. Startup needs to confirm its own identify and public key (often fails)
2. Startup of FreeS/WAN causes 30 seconds of DNS misses and packetloss
3. Application sends packet to remote host (eg www.nohats.ca)
4. Kernel intercepts packet, sends to IKE daemon
5. IKE daemon tries to find IPSECKEY/TXT record in reverse DNS
6. (meanwhile application retries initial packet, or fails loudly)
7. IKE daemon sets up IPsec tunnel
8. Application, if not given up, send packet through tunnel
9. (LOTS of 'failures' to remember in SPD/SAD on both sides)

The FreeS/WAN era problems and mistakes

- Ahead of its time (technically, politically)
- Only mutual authenticated IPsec - enduser must publish IPSECKEY (too hard)
- Key distribution via reverse DNS(SEC) which hasb een abandoned
- Hoped IPv6 would obsolete NATs
- Intercept packet, then find identity
- The common "no OE" fallback to plaintext took too long
- (later, supported initiator-OE and NAT-T)

What has changed?

- Pervasive monitoring - anonymous IPsec better than plaintext
- Deployed DNSSEC - possible to put validator on every device
- Devices powerful enough to do lots of IPsec and DNSSEC

What has NOT changed?

- Users are still not able to configure IPSECKEY in DNS
- Still no IPv6 host-to-host, but NATed client-to-server
- Reverse DNS still unusable

Opportunistic Encryption with IPsec

1. Application sends DNS request for A record (eg www.nohats.ca) to local DNSSEC resolver
2. DNS server attempts to find A record as well as IPSECKEY record for www.nohats.ca
3. If IPSECKEY record found, send IP address, FQDN and IPSECKEY to IKE daemon
4. IKE daemon sets up IPsec tunnel using (internet wide) PSK for its own authentication, RSA for remote auth.
5. DNS server returns A record to application
6. Application send data, automatically goes over IPsec tunnel

Anonymous OE with IPsec

1. Application sends DNS request for A record (eg www.nohats.ca) to local DNSSEC resolver
2. DNS server attempts to find A record as well as IPSECKEY record for www.nohats.ca
3. No IPSECKEY record found, send IP address, FQDN to IKE daemon
4. IKE daemon sends blind IKE attempt to remote IP with universal PSK. Works of fails.
5. DNS server returns A record to application
6. Application send data, automatically goes over IPsec tunnel if other end supported IKE.

Comparison with BTNS

- public keys / CERT exchanged inline only - no server authentication
- Connection latching, channel binding, upgrades, IKE policies, new SAD/SPD flags
- Requires async DNS lookups (or other async auths) in IKE daemon
- Does not use assymetrical IKEv2 authentication (PSK =¿ ¡= RSA) thus privacy leak
- Needs to generate ephemeral RSA keys which is bad for low entropy embedded gateways
- IKE daemon becomes complex - needs modification instead of configuration (¿3 lines of code)

Implementation details

Planned for Libreswan 3.7, tentatively in Fedora 21 and enabled per default in Fedora 22

- Deal with overlapping NAT using server-side NAT to 127.* addresses
- If both have published IPSECKEY, how to handle role reversal when starting as anonymous
- Reluctantly accept client-server versus host-host
- Combine OE with "static configurations" by simply using multiple policies (no modification)
- On Linux/BSD set OE IPsec "priority" field to be always lower than non-OE IPsec
- (What to do with IKEv1 old OE code - remove?)
- Keep kinds of OE connection to a minimum - no leap of faith IPsec