IETF 93 DPRIVE IPSEC

Using IPsec to encrypt DNS

(or do we really need a DNS protocol update?)

Paul Wouters
The Libreswan Project

Which DNS to encrypt?

- DNS at your home or office network?
  - Just encrypt everything using strong authenticated encryption
- Trusted external DNS server?
  - That's a just a pre-configured static (IPsec) VPN
  - No new IETF VPN protocols needed
  - (except if using DNSSEC to publish key, draft-ietf-nir-ipsecme-gateway-pubkey--1)
- Coffee shop DNS?
  - You trust the owner marginally more than fellow wifi inmates
  - No real point authenticating the DNS server
    - Authenticate StarBucksLocation43627543 ?
  - Why not just encrypt all traffic instead of only DNS?
    - DNS server is usually the network gateway for everything anyway

Use IPsec to auto-encrypt (DNS)

- Uses libreswan-3.14rc3 IPsec software
- About 10 lines of configuration
- Uses draft-ietf-ipsecme-ikev2-null-auth

How does it work?

- DNS plaintext packet is sent by DNS application (or local DNS server)
- IPsec kernel policy for DNS packets “traps” packet
  - Notification sent to IKE daemon
  - Packet causing trap is dropped
- IKE daemon attempts to establish IKE/IPsec
  - Installs negotiation shunt (leak or drop)
  - Uses host-to-host tunnel mode
  - Optionally limited to DNS traffic only
  - If success, negotation shunt replaced with IPsec encryption policy
  - If fail, negotiation shunt replaced with failure shunt (leak or drop)
  - When IKE or IPsec lifetime is reached, rekey if used else terminate

/etc/ipsec.conf for coffee wifi

```
conn private-or-clear
    left=%defaultroute
    right=%opportunisticgroup
    # leftprotoport=17/%any
    # rightprotoport=17/53
    authby=null
    leftid=%null
    rightid=%null
    ikev2=insist
    failureshunt=passthrough
    negotiationshunt=hold
    auto=ondemand
```

ipsec.conf for external trusted DNS

```
conn google-dns-with-ipsec
    left=%defaultroute
    right=8.8.8.8
    leftprotoport=17/%any
    rightprotoport=17/53
    leftauthby=null
    leftid=%null
    rightid=@dns.google.com
    rightauthby=rsasig
    ikev2=insist
    failureshunt=hold
    negotiationshunt=hold
    auto=ondemand
```

Why do we need DNS modifications?

- So no other VPN technology needed?
- It's kinda cool to do it in the DNS protocol?
- Not encrypted by me syndrome?

- Maybe for DNS recursor to authoritative DNS?

If DNS protocol modification are done, make it really simple or I will try to use IPsec instead :P