IKEv2 VPN with OpenBSD iked(8)

EuroBSDCon 2010-10-09, Karlsruhe

Reyk Flöter (reyk@openbsd.org)

Agenda

- Why another VPN protocol?
- Limitations of IKEv1 and isakmpd(8)
- Internet Key Exchange version 2 (IKEv2)
- Design & implementation of iked(8)
- The real world: running iked(8)

Why another VPN protocol?

- We have lots of existing VPN protocols:
  - IPsec IKEv1 with isakmpd(8)
  - L2TP, PPTP and more with npppd(8)
  - OpenSSH (SSH-VPN with tun(4))
  - OpenVPN in ports...
- And many vendor-specific SSL-VPNs
  - Microsoft's SSTP: PPP over HTTPS
  - Cisco AnyConnect, Juniper, Citrix, ...

Why another VPN protocol?

- Different VPN types for different use cases
  - SSL-VPN: lots of overhead but passes web proxies; different protocols
  - IPsec: does a better job on IP but IKEv1 is less flexible with NAT and mobility
  - OpenVPN: for religious people
  - BGP MPLS VPN: large virtual networks but without privacy (it should be "VN")
- We need a standardized, widely adopted, secure, flexible and low-overhead protocol

IKEv1 and ISAKMP/Oakley

- IKE? ISAKMP? Oakley? DOI?
  - Internet Key Exchange; RFC 2409
  - on top of ISAKMP/Oakley; RFC 2408
  - on top of the Internet DOI; RFC 2407

  + many addtitonal RFCs
- Widely adopted and (mostly) interoperable
  - Cisco, racoon, strongswan, Windows, ...
- Long history with strong security research
  - Known weaknesses, do's and dont's

isakmpd(8)

- Written 1998 by Niklas Hallqvist and Niels Provos for Ericsson
- Supports the full ISAKMP and DOI layering
  - but IKE is the only protocol on top of it
- Uses an .ini-style configuration (yay '98)
  - And the KeyNote policy language
- Does not support some of the extensions
  - No XAUTH (user/password), No IKECFG
- Doesn't work very well with roadwarriors

ipsec.conf(5) and ipsecctl(8)

- Workaround isakmpd to make it useable
  - The daemon is ok, but the useability...
- ipsec.conf is a nice config grammar that will be loaded into isakmpd.fifo by ipsecctl
  - Benefit: you don't need to touch the .ini and the KeyNote policy anymore
  - Problems: Two steps to run isakmpd
    - isakmpd -K && ipsecctl -f ipsec.conf
    - Doesn't do reloads - kill & restart

Internet Key Exchange version 2 (IKEv2)

- They learned a lesson and simplified IKE
  - No ISAKMP+DOI layers anymore
  - The IKEv2 payload is now like ESP
- One 4-way handshake, optional cookies
- Improved network robustness and mobility
  - Even PSK works with roadwarriors now
- New concept of traffic selectors (flows)
  - IKEv1 embedded the flows in the ID
- RFC 4306 by Microsoft (surprise)

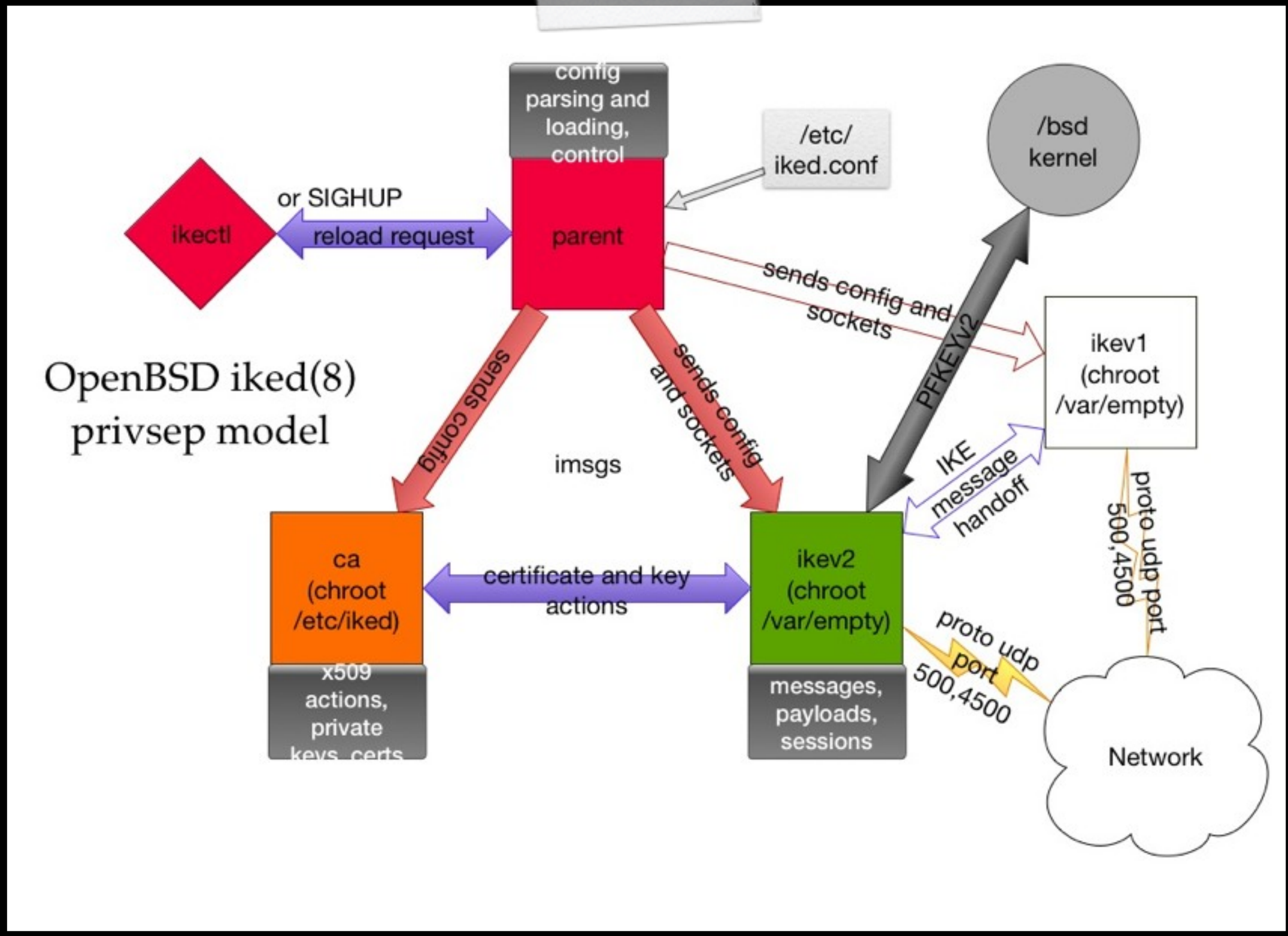
Internet Key Exchange version 2 (IKEv2)

- A quick reference:
  - Traffic Selectors: One or more flows per IKEv2 SA (from x.x.x.x to y.y.y.y)
  - IKESA: formerly known as Phase 1
  - CHILDSA: Phase 2 for IPsec ESP/AH
  - Initiator: the client
  - Responder: the server
  - PRF: pseudo-random function
  - EAP: Extensible Authentication Protocol

iked(8)

- A new implementation of IKEv2; RFC 4306
- Based on the following design decisions:
  - A privsep'd daemon for OpenBSD
  - An integrated ipsec.conf-style config
  - Stateful config reloads
  - Control with ikectl(8) **not** isakmpd.fifo
  - Scalable with gw2gw and roadwarriors
  - Provide better X.509 CA useability
  - Use OpenSSL instead of custom crypto

Design & implementation of iked(8)



All kinds of strong crypto

- Modern ciphers for IKESA and CHILDSAs
  - eg. Auth & PRF with SHA2
  - More AES modes (CBC, CTR, GCM)
  - More Diffie-Hellman modes
    - 26 groups, up to modp8192, ecp521
    - Elliptic curve groups are fast and secure
- Supports authenticated encryption
  - AES-GCM support added by Mike Belopuhov (mike@openbsd.org)

ikectl ca

- Manage a simple X.509 CA for iked
  - Simple configuration of certificates

1. ikectl ca test create
2. ikectl ca test install
3. ikectl ca test cert 10.1.1.1 create
4. ikectl ca test cert 10.1.1.1 install
5. ikectl ca test cert 10.1.1.2 create
6. ikectl ca test cert 10.1.1.2 export

MOBIKE and other future work

- Finish the basic IKEv2 support
  - We don't initiate rekeying yet... oops
  - Cleanup, fixes, serious reviews
- MOBIKE improves mobility support by allowing peers to update existing SAs after their external IP address changed
  - We want to support RFC 4621
- Implement RADIUS support to tunnel all other EAP types.
- Revised IKEv2 RFC 5996 from Sep 2010

The real world: running iked(8)

- We tested it so far with:
  - Windows 7: really easy to set up!
  - Linux Strongswan: *narf*
- Soon:
  - Cisco IOS & AnyConnect 3
  - Not-so-OpenSolaris
- Want to try?
  - ikectl ca...
  - mg /etc/iked.conf && iked

Danke!

...and thanks for supporting the OpenBSD project!