DHCP-over-IKE

Michael Richardson
<mcr@sandelman.ottawa.on.ca>
Sandelman Software Works Corporation

Requirements

□ do not reinvent name spaces

□ provide client with all info it needs

□ takes as few exchanges as possible (counting IPsec SAs too!)

□ interfaces to existing infrastructure: DHCP, RADIUS, (new ones)

□ optionally preserves possible end-to-end security in DHCP

□ permits independant evolution of DHCP

□ out-of-scope: IPv6 (for now)

Three methods

- DHCP-over-IPsec
- ModeCFG-over-IKE
- proposed - DHCP-over-IKE

DHCP-over-IPsec

- □product of IPSRA
- □make temporary 0.0.0.0/0<->0.0.0.0/0 SA for DHCP
- □simple for Bump-In-the-Stack
- □easy for all-in-one gateways
- □leverages existing DHCP server

ModeCFG

- occurs in IKE, during message 3
- uses custom payload
- if you need DHCP info, you do it over IPsec SA
- easy to interface to radius/COPS/AAA/etc.

Why another

- DHCP is *the* method for configuring systems
- we should not invent new things here

DHCP-over-IKE vs DHCP-over-IPsec

- creating 0/0<->0/0 is VERY hard when crypto is offloaded
- client systems without virtual interfaces save no dhcp client code
- may have to leave 0/0 around for renewals
- gives some people the willies

DHCP-over-IKE vs ModeCFG

- modecfg is the same as DHCP-over-IKE, except for format of bits
- DHCP-over-IKE had a exchange 1.5, but can deal with this (maybe)
- DHCP-over-IKE preserves client<->server security (RFC3118)
- naturally extensible (just lean on DHC WG)
- can plug into Radius/COPS with mini-DHCP server/proxy
- talks to real DHCP server with no glue (very widely deployed)

Recent changes

- proposed that we eliminate DHCPOFFER/DHCPREQUEST messages
- if real DHCP server, server may deal with them
- gets rid of exchange 1.5 when no RFC3118
- leave exchange 1.5 in when RFC3118