IPsec: IP security in opensource systems

Pavel Šimerda
pavlix@pavlix.net

IPv6 Day 2012, Praha

http://data.pavlix.net/ipv6day/2012/

Contents

- IP Security Overview
- Kernel IPsec implementation
- Comparison of Key Exchange Implementations

IP Security Overview

IPsec

- IP Security $\longrightarrow$ IPsec
- Mandatory part of IPv6 stack, extension to IPv4 stack
- Network-layer packet encryption and authentication

IPsec provides

- Security layer for network and transport protocols
- Data authentication, integrity and confidentiality
- Mutual host and user authentication
- Security orthogonal to routing (with public IPv6 or IPv4)
- End-to-end secure communication (with public IP and DNSSEC)

IPsec essentials

- Security policy database
- Security association database
- Encapsulated security payload
- Key exchange and configuration

Kernel IPsec Implementation

Kernel part

- Linux style versus BSD style
- Runtime configuration tools (ip, setkey)
- Firewall configuration

ESP transport channel

- Mode: Transport
- Encapsulation: IPv6–ESP
- Direction: alpha.example.net → beta.example.net
- Addresses: `2001:db8::a` → `2001:db8::b`
- Use the same commands for the reverse channel
- Suitable for secure end-to-end connectivity

ESP transport channel

ICMP ping from alpha to beta

```
# ping6 2001:db8::b
PING 2001:db8::b(2001:db8::b) 56 data bytes
64 bytes from 2001:db8::b: icmp_seq=1 ttl=255 time=0.630 ms
64 bytes from 2001:db8::b: icmp_seq=2 ttl=255 time=0.504 ms
```

Network traffic (tcpdump)

```
IP6 2001:db8::a > 2001:db8::b:
        ESP(spi=0x00000001,seq=0x1), length 104
IP6 2001:db8::b > 2001:db8::a:
        ICMP6, echo reply, seq 1, length 64
IP6 2001:db8::a > 2001:db8::b:
        ESP(spi=0x00000001,seq=0x2), length 104
IP6 2001:db8::b > 2001:db8::a:
        ICMP6, echo reply, seq 2, length 64
```

ESP tunnel

- Mode: Tunnel
- Encapsulation: IPv6–ESP–IPv6
- Routers: `2001:db8::a` → `2001:db8::b`
- Networks: `2001:db8:a:a::/64` → `2001:db8:b:b::/64`
- Use the same commands for the other direction
- Suitable for secure links between two networks

Hybrid IPv6/IPv4 ESP tunnels

- Mode: Tunnel
- Encapsulation: IPv4–ESP–IPv6 or IPv6–ESP–IPv4
- Use the same commands as for IPv6–ESP–IPv6 tunnels
- Use IPv4 network or host addresses where appropriate
- Suitable for secure IPv4 links between IPv6 networks and vice versa

Comparison of Key Exchange Implementations

The IKE protocol

- Dynamic security policies and associations (including keys)
- On-demand associations
- Mutual authentication using PSK, PKI or other mechanisms

IKEv1

- Multiple initial exchange modes
- Cryptographic weaknesses

IKEv2

- Fusion of previous specifications
- Single initial exchange mechanism
- Improved cryptography and unified with ESP
- Improved remote network configuration
- Improved NAT-T support

IKE implementations in Fedora/EPEL

- Racoon
- Openswan
- Racoon2
- Strongswan

There may be others. For example vpnc seems to be a specialized IPsec implementation used as a client to Cisco EasyVPN.

Racoon (ipsec-tools)

- Included in Linux distributions, FreeBSD and NetBSD
- Limited to obsolete IKEv1
- Very hard to configure for advanced scenarios
- Even road warrior scenario requires shell scripting
- It seems to support IPv6 except hybrid tunnels

Openswan (tested with 2.6.33)

- Included in Linux distributions including RHEL
- Probably supports FreeBSD/NetBSD
- Broken links and lack of information on homepage
- IKEv2 doesn't work with NAT traversal
- IKEv2 doesn't work in road warrior setup
- IPv6 doesn't work in road warrior setup
- IPv6 configuration and errors are confusing
- Hybrid tunnels aren't supported
- Openswan gets confused by multiple IPs per interface

Racoon2

- In some distributions (Fedora, EPEL), support for FreeBSD/NetBSD
- Latest version from May 2010
- Rather complicated configuration, but *very* flexible
- Ready-to-use configuration examples
- Reportedly decent IKEv2, IKEv1 and IPv6 support

Strongswan

- Included in Linux distributions, support for FreeBSD
- Problems in older versions (in stable distributions)
- Active upstream, new release every few months
- IKEv2, IKEv1 and IPv6 support including hybrid tunnels
- NAT-T, Mediation, MOBIKE and virtual IP support
- Various authentication mechanisms
- Easy and almost flat configuration, similar to Openswan

Choosing an IKE implementation for IPv6

Requirements

- IKEv2 and IKEv1 support
- Support for IPv6 and hybrid IPv4/IPv6 tunnels
- Road warrior setup
- IPv4 NAT traversal
- All of the above working together

Evaluation

- Racoon – not suitable, lacks IKEv2
- Openswan – not suitable, broken IKEv2 as well as IPv6
- Racoon2 – suitable, passive development, complicated setup
- Strongswan – suitable, actively developed, straightforward setup

Questions?

http://data.pavlix.net/ipv6day/2012/

pavlix@pavlix.net