ike Documentation

Release 0.0.3

Kimmo Parviainen-Jalanko

April 08, 2014

Contents:

CHAPTER 1

About ike

The goal of this project is to be a minimalistic IKEv2 (RFC 5996) implementation in Python.

1.1 Status

This project is in early stages. Use at own risk.

It will make your IP stack talk ESP to the remote peer.

What it can do:

- Act as an initiator
- Authenticate itself and peer using raw RSA keys.
- Install ESP SAs and SPD entries to use the key material via `setkey` command from ipsec-tools.

Limitations (hardcoded values):

- Cipher algorithm is Camellia in CBC mode with 256 bit keys.
- HMAC / Hash / PRF algorithm is SHA2/256.
- IKE group is Diffie-Hellman modp 14.
- Authentication (both own private and peer public) key file paths are hardcoded.
- 'setkey' syntax is of whatever the ipsec-tools on Debian 7.1 accept.
- Traffic selectors are myip:any:0-65535 <-> peerip:any:0-65535

1.2 Design principles

- Minimal amount of code.
- Support *MUST* features of draft-kivinen-ipsecme-ikev2-rfc5996bis-02 (RFC 5996 successor)
- Use strongest algorithms possible.

1.3 Documentation

You can read the Documentation at https://ike.readthedocs.org

1.3.1 What this project is *NOT* going to be

- ISAKMP (IKEv1) RFC 2409 compliant
- IPSec data plane / ESP protocol

1.4 License

- MIT License

1.5 References

- http://tools.ietf.org/html/draft-kivinen-ipsecme-ikev2-rfc5996bis-02
- http://tools.ietf.org/html/draft-kivinen-ipsecme-ikev2-minimal-01

CHAPTER 2

ike package

2.1 Subpackages

2.1.1 ike.util package

Submodules

ike.util.cipher module

ike.util.conv module

ike.util.dh module

ike.util.dump module

ike.util.external module

ike.util.prf module

ike.util.pubkey module

Module contents

2.2 Submodules

2.3 ike.const module

2.4 ike.initiator module

2.5 ike.payloads module

2.6 ike.proposal module

2.7 ike.protocol module

2.8 Module contents

CHAPTER 3

ike

3.1 ike package

3.1.1 Subpackages

ike.util package

Submodules

ike.util.cipher module

ike.util.conv module

ike.util.dh module

ike.util.dump module

ike.util.external module

ike.util.prf module

ike.util.pubkey module

Module contents

3.1.2 Submodules

3.1.3 ike.const module

3.1.4 ike.initiator module

3.1.5 ike.payloads module

3.1.6 ike.proposal module

3.1.7 ike.protocol module

3.1.8 Module contents

CHAPTER 4

Indices and tables

- *genindex*
- *modindex*
- *search*