

Features

- Seamlessly integrates hardware offload into Linux IPsec
- Supports IPv4 IPsec PDU processing hardware offload
 - Replacement of fast path ESP/AH function with hardware
- Supports IPv6 IPsec hardware offload
 - Replacement of fast path cipher operations with hardware
- Reference code licensed in C Source Code
- Developed for Linux Fedora Core 6 with the 2.6.22 kernel
- FPGA based evaluation platform available with the EVAL-01 Evaluation Card

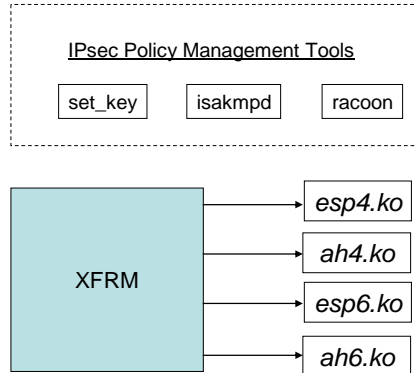
The ESS-03 is part of the Ellipsys Security Architecture (ESA) which offers a comprehensive set of security software for embedded applications. The ESS-03 offers a reference design for integrating any of the CLP-25, CLP-30 or CLP-36 ESP/AH Offload Engines into Linux IPsec.

Linux IPsec is a robust, open platform that has been widely adopted by embedded software developers. The challenge in integrating hardware offload has been finding the optimum method of substituting hardware offload function for software processes. The ESS-03 facilitates an offload solution for both IPv4 and IPv6 implementations of IPsec and is available in C source code to speed time to market through a complete reference solution from Elliptic.

General Description

Overview of Linux Kernel IPsec

The Linux IPsec functionality is integrated into the native TCP/IP stack.



The IPsec implementation consists of a transformation engine (XFRM) and loadable ESP and AH modules. XFRM also provides SADB lookup infrastructure. The loadable modules make the IPsec environment very easy to customize. When loaded a module registers specific entry points to appropriate functions during initialization.

The CLP-25 and CLP-36 hardware cores offer hardware packet processing for IPv4 IPsec and crypto offload of cipher and hashing for IPv6 based implementations of IPsec. For implementations using IPv6 IPsec, the offload is offered through crypto processing of individual algorithms such as AES and 3DES.

For IPv6 ESP processing, the CLP-25 or CLP-36's IPv4 ESP mode can also be used to achieve higher performance cipher and hash processing by manipulating the header structures and SA records before and after processing the packet.

ESS-03 Linux IPsec Reference Middleware

The Elliptic Linux IPsec reference implementation has been transparently integrated into the Linux kernel. This means the ESP and AH kernel modules for IPv4 IPsec are functionally identical and replace the corresponding native modules, providing identical SA management and packet flow functions. The following table outlines the module substitution map:

Native Module	Elliptic Module	Description
esp4.ko	elpeesp4.ko	IPv4 ESP Protocol Module
ah4.ko	elpah4.ko	IPv4 AH Protocol Module
esp6.ko	elpeesp6.ko	IPv6 ESP Protocol Module
ah6.ko	elpah6.ko	IPv6 AH Protocol Module
N/A	elpepah.ko	CLP-25/CLP-36 IPsec interface module
N/A	elcrypto.ko	CLP-25/CLP-36 Crypto interface module

General Description cont'

For Linux IPsec implementations that require support for IPv6, the ESS-03 substitutes hardware hashing and cipher capabilities for the software code used in the standard solution. The ciphers and hashes available for substitution are based on the algorithms available in the CLP-25 or CLP36 engines and include AES-CBC, 3DES, HMAC/SHA-1 and HMAC/MD5 functions.

Customers interested in building a lab prototype of the combined hardware and software solution can do so using the ESS-03 along with the EVAL-01 Evaluation System.

Ellipsys Security Architecture

The Ellipsys Security Architecture consists of five distinct products encompassing symmetric and asymmetric cryptography primitives, secure boot, Linux IPsec and DTCP stack.

The architecture offers a well defined, uniform API blending industry standard PKCS#11 and PKCS#5 compliance with proprietary extensions in support of third party applications software, the ability to choose between hardware and software security primitives and platform security elements such as secure boot and key management.

When used with Elliptic hardware, a wide variety of use models are available supporting single crypto cores all the way up to sophisticated packet processing engines.

The Ellipsys Security Architecture can also be adapted to hardware offload in off the shelf processors with board support packages (BSPs) written either by Elliptic or by customers themselves. Ellipsys is written to be highly portable and is licensed in C source code. The Ellipsys Security Architecture is illustrated in the figure below.

Ordering Information

- Offered in highly portable source code format, the ESS-03 is available for immediate licensing.

