**Overview**

Cryptodev-linux is a device that allows access to Linux kernel cryptographic drivers; thus allowing of userspace applications to take advantage of hardware accelerators. Cryptodev-linux is implemented as a standalone module that requires no dependencies other than a stock linux kernel. Its API is compatible with OpenBSD's cryptodev userspace API (/dev/crypto).

**Features**

* Self contained linux kernel module
* Exact simulation of the /dev/crypto interface
* Support for all major cipher and hash algorithms
* Zero copy of data
* Support for additional features to optimize TLS and SRTP protocols
* Support for AEAD ciphers
* Asynchronous and synchronous interfaces

**Why use /dev/crypto**

Several small systems include a hardware crypto device that optimizes cryptographic operations with a 100x factor or even more comparing to a plain software implementation. Those systems usually provide kernel space drivers for those accelerators but they are not accessible from typical usespace programs and libraries such as [GnuTLS](http://www.gnutls.org/) or [OpenSSL](http://www.openssl.org/). The /dev/crypto device is a middleware allowing access to the hardware cryptographic modules from user-space applications and thus providing cryptographic operations acceleration.

**Why use cryptodev-linux**

* It provides [better performance](http://cryptodev-linux.org/comparison.html) than any of the alternatives including AF\_ALG;
* It has an API-compatible interface with FreeBSD and OpenBSD cryptodev;
* It uses the native Linux kernel crypto drivers.

**Alternatives**

* [NCR](http://cryptodev-linux.org/ncr.html) a Cryptographic Framework for Linux originally based on this one. Instead of simply providing cryptographic operations, it acts as a software security module.
* [OCF-linux](http://ocf-linux.sourceforge.net/) is a port of the OpenBSD Cryptographic Framework to Linux that also includes the /dev/crypto interface. This unlike cryptodev-linux does not use the native Linux crypto interfaces.
* [Linux 2.6.38 AF\_ALG](http://lwn.net/Articles/410536/). Linux 2.6.38 introduced a sockets-based protocol to perform cryptographic operations. It is very inefficient in modern hardware; we made a performance [comparison with cryptodev-linux](http://cryptodev-linux.org/comparison.html).

The following tests benchmark the speed of initialization, encryption and deinitialization of the cipher.

|  |  |
| --- | --- |
| http://cryptodev-linux.org/cesa-full.png | http://cryptodev-linux.org/crypto-afalg-null.png |
| Throughput of the cbc(aes) cipher (CESA) | Throughput of the ecb(cipher-null) cipher |

The following benchmarks show the speed of encryption of the cipher. This does not include the initialization phase of the cipher (key expansion), but only the time spent for encryption.

|  |  |
| --- | --- |
| http://cryptodev-linux.org/cesa-enc-only.png | http://cryptodev-linux.org/enc-only-null.png |
| Throughput of the cbc(aes) cipher (CESA) | Throughput of the ecb(cipher-null) cipher |