Disk Encryption with 100GbE Crypto Accelerator

Chelsio T6 vs. Intel AES-NI vs. Software Enabled Encryption

Executive Summary

Chelsio Crypto Accelerator is a co-processor designed specifically to perform computationally intensive cryptographic operations more efficiently than general-purpose CPUs. Servers with system load, comprising of cryptographic operations, see great performance improvement by offloading crypto operations on to the Chelsio Unified Wire adapter. Chelsio's solution uses the standard crypto API framework provided by the operating system and enables the offloading of crypto operations to the adapter.

This paper showcases the disk encryption acceleration capabilities of Chelsio T6 adapters by comparing its performance with Intel AES-NI and software encryption. Chelsio solution excels with 100Gbps Crypto rate performance for both encryption and decryption with less than 50% CPU usage. Chelsio's T6 encryption solution assures complete data protection to datacenters, while providing substantial savings on CPU and memory.

Chelsio Disk Encryption Offload

The Terminator 6 (T6) ASIC from Chelsio Communications, Inc. is a sixth generation, high performance 1/10/25/40/50/100Gbps unified wire engine which offers crypto offload capability for AES and SHA variants. Chelsio's disk encryption solution is a special case of *data at rest* protection where the storage media is a sector-addressable device. Chelsio offloads the AES-XTS mode, which is designed for encrypting data stored on hard disks where there is no additional space for an integrity field. AES-XTS builds on the security of AES by protecting the storage device from many dictionary and copy/paste attacks. Chelsio crypto driver registers with the kernel crypto framework with high priority and ensures that any disk encryption request is offloaded and processed by T6 adapter. Block device encryption methods operate *below* the filesystem layer and make sure that everything written/read from block device is encrypted/decrypted.

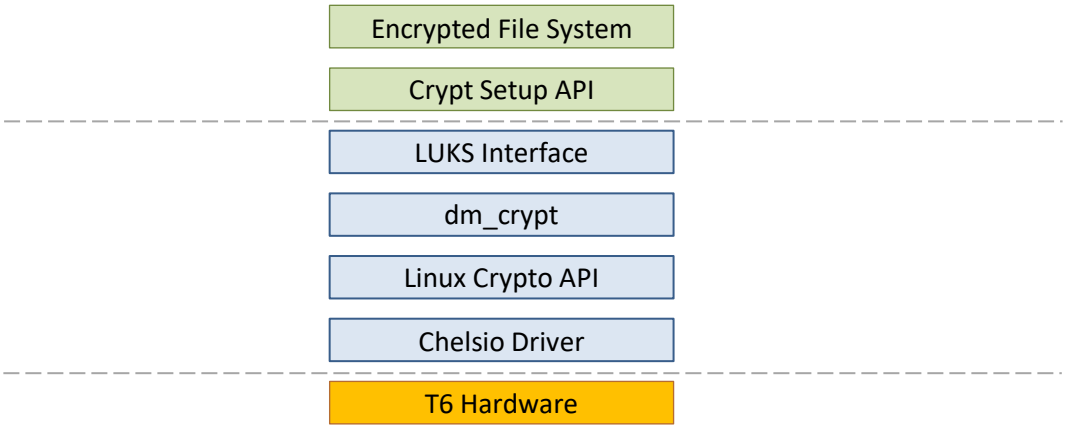

Figure 1 – T6 disk encryption Acceleration

Test Results

The following tables show the encryption and decryption rate, CPU Usage with Chelsio crypto (offload), Intel AES-NI and software crypto (non-offload) modes using the **cryptsetup** tool.

Mode	Encryption rate (Gbps)	Decryption rate (Gbps)	CPU usage (%)
Chelsio crypto	95.605	95.591	47.8
Software-crypto	15.699	16.001	99.75

Table 1 - Chelsio crypto vs. Software Encryption

Chelsio crypto solution delivers upto 6x the performance in Software mode, reaching 95Gbps Crypto rate for both encryption and decryption. Additionally, with 50% savings in CPU utilization, Chelsio crypto solution indicates a more efficient processing path.

Mode	Encryption rate (Gbps)	Decryption rate (Gbps)	% CPU	%CPU/Gbps
Chelsio crypto	95.605	95.591	47.8	0.5
Intel AES-NI	123.616	128.565	99.75	0.75

Table 2 - Chelsio crypto vs. Intel AES-NI

Comparing with Intel AES-NI, Chelsio crypto solution shows up to 30% reduction in CPU usage per Gbps freeing up precious CPU cycles for use by other applications. Intel AES-NI completely exhausts the CPU leaving no room for other applications.

Test Configuration

The setup consists of a machine configured with 1 Intel Xeon CPU E5-1660 v2 6-core processor clocked at 3.70GHz (HT enabled), 32GB of RAM and RHEL 7.3 operating system (kernel 4.9.13). Chelsio T62100-CR adapter was installed in the system and configured with Co-processor Driver v1.0.0.0. cryptsetup rpms (cryptsetup-libs-1.7.2-1.el7.x86_64.rpm and cryptsetup-1.7.2-1.el7.x86_64.rpm) were installed.

Setup Configuration

i. Install the driver package.

```
[root@host ~]# ./install.sh -i
```

ii. Reboot the machine into newly installed kernel.

iii. Install Chelsio Crypto accelerator driver.

```
[root@host ~]# ./install.sh -d
```

iv. A disk was created using RAM:

```
[root@host ~]# modprobe brd rd_nr=1 rd_size=4000000
```

v. A cryptographic device mapper device was created in LUKS encryption mode

```
[root@host ~]# cryptsetup -v luksFormat --cipher="aes-xts-plain64" /dev/ram0
```

vi. The partition was unlocked. Here *map* is device mapper name.

```
[root@host ~]# cryptsetup open --type luks /dev/ram0 map
```

vii. The disk was formatted and mounted.

```
[root@host ~]# mkfs.ext3 /dev/mapper/map
[root@host ~]# mount /dev/mapper/map /mnt/
```

viii. Respective drivers were loaded for Chelsio crypto and Intel AES-NI modes. No drivers required for Software mode.

Chelsio Crypto:

```
[root@host ~]# modprobe -v chcr
[root@host ~]# ifconfig <ethX Chelsio Interface> up
```

Intel AES-NI:

```
[root@host ~]# modprobe aesni_intel
```

ix. *cryptsetup* tool was run:

```
[root@host ~]# cd /mnt/
[root@host mnt]# for i in `seq 0 23`; do cryptsetup benchmark --cipher="aes-xts-plain64" & done
```

Conclusion

This paper presented performance comparison of Chelsio's T6 disk encryption acceleration solution using T62100-CR adapter. With encryption and decryption performance of more than 95Gbps and less than half the CPU usage, Chelsio crypto solution clearly outperforms both Intel AES-NI and software enabled encryption.

As more and more information is digitized and transmitted using computer networks, the need to safely store and transfer sensitive information has become the topmost priority for most datacenters. Chelsio's Terminator 6 (T6) Unified Wire adapters enable concurrent secure communication and secure storage with support for integrated TLS/SSL/DTLS and inline cryptographic functions, leveraging the proprietary TCP/IP offload engine for acceleration. Without the need for separate infrastructure and third-party software, Chelsio provides a low-power, low-cooling, low-cost encryption acceleration along with big savings on processing power and memory.

Related Links

Apache TLS/SSL Acceleration at 100GbE
Accelerated IPsec-VPN Communication with T6
T6 100GbE Crypto Offload Performance
Chelsio Terminator 6 ASIC 100GE Crypto Offload
The Chelsio Terminator 6 ASIC
Chelsio T6 Crypto Offload Video
Dm-crypt documentation