interopLab

Bloombase Cryptographic Module Benchmarking

BLOOMBASE®

Tests in this report are carried out with support and sponsor of Advanced Micro Device Inc.

Document No.

Contents

Contents 3

Overview 4

Bloombase Cryptographic Module 6
Introduction 6
Engine Throughput Test 6
Setup 7
Results 8
Conclusion 8

Overview

Cryptography is commonly perceived as shuffling and coding of data which is wrong. Data shuffling refers to the process of altering the order of sequence of data in a systematic way. By reversing the disordering process, one regains the original contents. Obfuscation is a coding process of data against a pre-defined look-up table. Again, obfuscation can be undone if one gets hold of the contents of the look-up table.

Cryptography is comparatively much complicated than both data shuffle and obfuscation described above. Cryptography originates from the good old idea of key-and-lock to secure precious objects inside a compartment. Similarly, cryptography requires a pre-generated key which is a series of random data resembling ridges of a physical key while the mathematical operation – the cipher, resembling mechanics of a physical lock, a transfer function of both key and data-to-be-secured which turns confidential data (precious objects) into a meaningless vault (secured compartment).

Numerous ciphers have been invented, a few examples are Blowfish, RC2, DES, 3DES and AES, etc. They differ in the algorithmic process, key length requirement, strength, complexity, ease of hardware implementation, resource requirement, ability to work with streamed data, performance and efficiency. Regardless of level of cipher efficiency and cryptographic processing engine performance, cryptographic operations – encryption and decryption, must add a relatively amount of time in the course of storage network data communications.

This document quantifies and summarizes the cryptographic throughput of Bloombase Spitfire Cryptographic Module which is the core building component of Spitfire family of security servers.

Bloombase Cryptographic Module

Introduction

This section of test aims to examine the maximum processing capacity of Bloombase Spitfire Cryptographic Module which is the main building block of entire Spitfire Security Platform. Spitfire Core Encryption Engine is a well-tuned and highly-optimized cryptographic software core which executes on Spitfire family of security servers.

Engine Throughput Test

A manufacturer's engine throughput test is carried out on Bloombase Spitfire Cryptographic Module loaded onto a dual-AMD Opteron dual-core processor grid to obtain the maximum cryptographic processing power of the unit.

Regardless of application, storage devices, protocol, transmission media and transmission interfaces, multiple endless streams of random data are generated and fed into a Bloombase Spitfire Cryptographic Module for encryption and decryption using Advanced Encryption Standard (AES) cryptographic cipher by randomly generated 256-bit symmetric key.

Setup

The following diagram shows the setup of this test. A Spitfire Core Encryption Engine is installed onto a system running on Spitfire OS which is a hardened and customized Linux of kernel version 2.6.11. Multiple plain random data streams are fed into for processing.

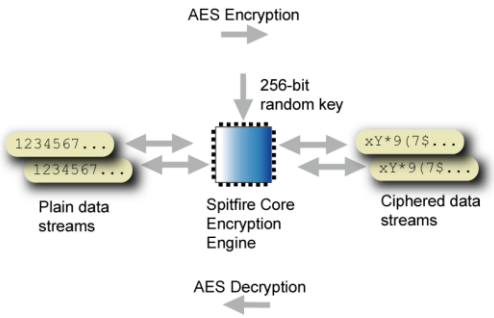

Figure – Setup of cryptographic processing performance tests on Bloombase Spitfire Cryptographic Module

The following table summarizes the hardware configuration of Spitfire cryptographic appliance

Processing Unit	Dual AMD Opteron dual-core 265 with true 64-bit support
Main Memory	2 GB
Persistence Storage	4 GB Flash
Operating System	Spitfire OS – Hardened and customized OS based on embeded Linux of kernel version 2.6.11

Security specific setup is as follows

Bloombase Spitfire Cryptographic Module	Version 2.0
Encryption Algorithm	Advanced Encryption Standard (AES) Cipher Block Chaining (CBC)
Encryption Key	Software only
Key Length	256-bit
Number of Random Data Streams	4
Cryptographic Tasks	• encryption • decryption

Spitfire Core Encryption Engine actively pulls in random data from input stream which is a random number generator. Ciphered data are outputted and encryption throughput is measured simply as the ensemble of ciphered data output rates.

Decryption performance tests, on the other hand, require more sophisticated technique because input data are supposedly ciphered data which cannot be randomly generated, or decryption will fail immediately due to unexpected runtime errors. To enable data be decrypted without error, ciphered data previously outputted as results of encryption are temporarily stored on memory. Decryption process intakes ciphered input from memory and again, decrypted output data rate measured and summed yielding overall decryption throughput rate.

Results

10 rounds of encryption and decryption tests are carried out successfully without error and throughput measured and averaged.

Results are summarized in below table

Encryption (Gbps)	Decryption (Gbps)
4.8119	4.7213

Results are plotted as follows

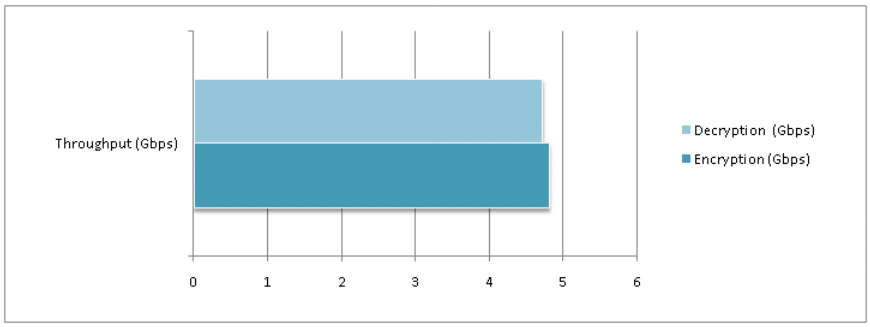

Figure – Bloombase Spitfire Cryptographic Module Net Processing Throughput

Encryption and decryption both run at gigabit speed

Encryption performs a little better (approximately 5%) than decryption

Conclusion

- Spitfire Cryptographic Encryption Engine running on dual AMD-Opteron module can encrypt and decrypt at rates of the same order of magnitude as current storage network communications speeds (1 Gbps, 4 Gbps, 8 Gbps

and 10 Gbps). For applications running on 4 Gbps storage systems at full speed, ideally, the engine may barely become the bottleneck

- Even though later application tests are built on storage network hardware operating at maximum 4.8 Gbps, there is slim chance an application can fully utilize the entire bandwidth in actual use. As Bloombase Spitfire Cryptographic Module's maximum throughput is still close to this speed, one can still claim such bottleneck effect should not be dominant in the tests follow

- To cater for next generation TCP/IP networking which operates at 40 Gbps and above, one might need to increase the processing power of the appliance by installing more processors to raise the overall cryptographic capability and further relieve the encryption bottleneck