How to check if AES-NI is enabled for OpenSSL on Linux

Author : Dan Nanni

Categories : Hardware, Security

Tagged as : aes, encryptionopenssl

Question: I have a Linux server which has Intel AES-NI hardware capability. I would like to check whether currently installed OpenSSL can use AES-NI acceleration.

Intel Advanced Encryption Standard New Instructions (AES-NI) is a special instruction set for x86 processors, which is designed to accelerate the execution of AES algorithms. AES-based symmetric encryption is widely used in a variety of security applications and protocol implementations (e.g., IPSec, SSL/TLS, HTTPS, SSH). OpenSSL crypto library supports AES-based ciphers as well.

To support AES-NI, OpenSSL provides so-called EVP crypto APIs (e.g., EVP_Decrypt/EVP_Encrypt) which can automatically leverage hardware acceleration (if available) and fall back to software implementation (if not available), via a single interface. If you want to check whether currently installed OpenSSL supports AES-NI hardware acceleration, you can test using OpenSSL's EVP APIs.

Check if AES-NI is Available on CPU Processors

Before proceeding, first verify that current CPUs have the AES instruction set. For this you can inspect CPU flags as follows.

```
$ grep -m1 -o aes /proc/cpuinfo
```

```
aes
```

If the output shows `aes`, that means AES-NI engine is available on current CPUs.

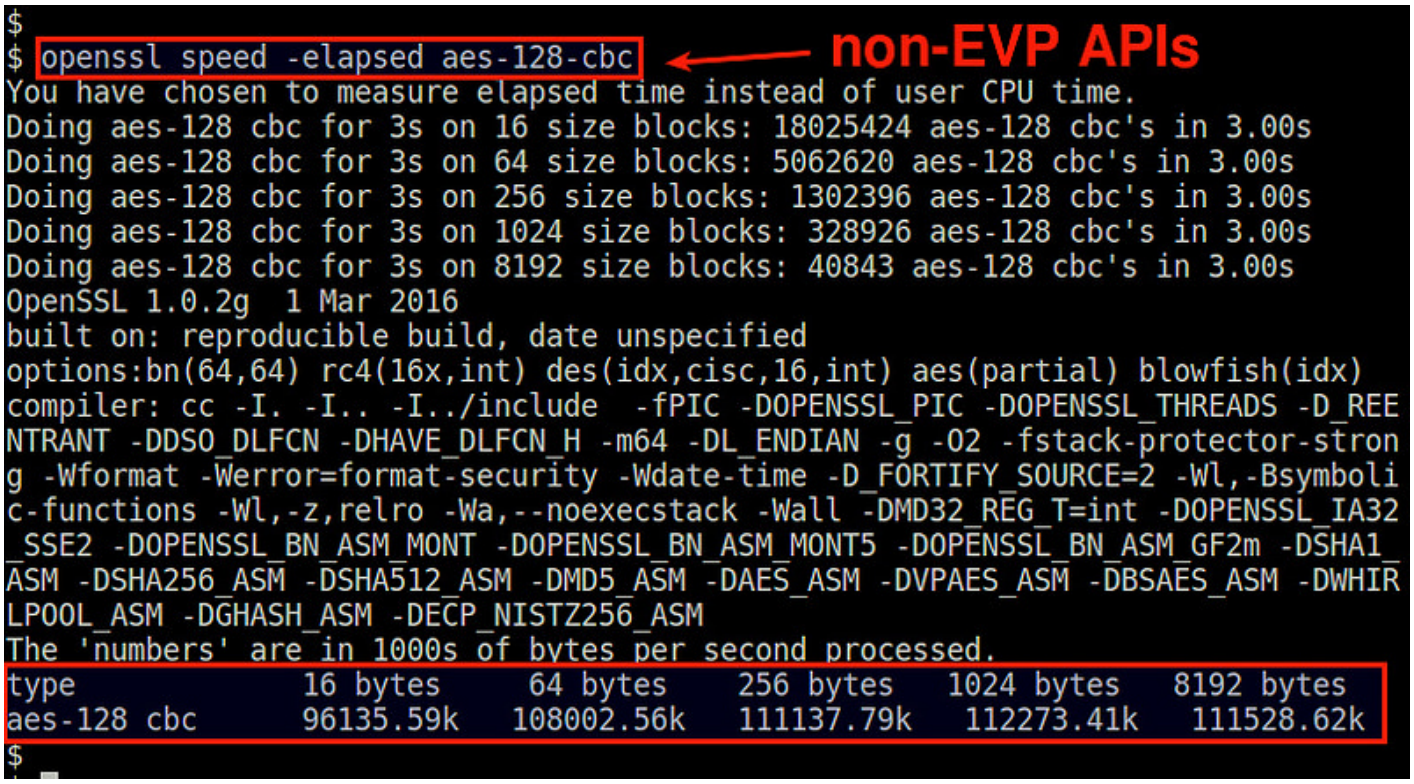
Check if AES-NI is Enabled for OpenSSL

To check whether OpenSSL can leverage AES instruction sets, you can use OpenSSL's EVP APIs. When EVP APIs are called, they can automatically detect the presence of AES-NI and accelerate AES encryption computations using AES instruction sets. Thus you can compare AES performance with or without EVP functions. If AES-NI is available for OpenSSL, you will see significant performance boost when EVP functions are used.

Let's use OpenSSL's built-in speed test.

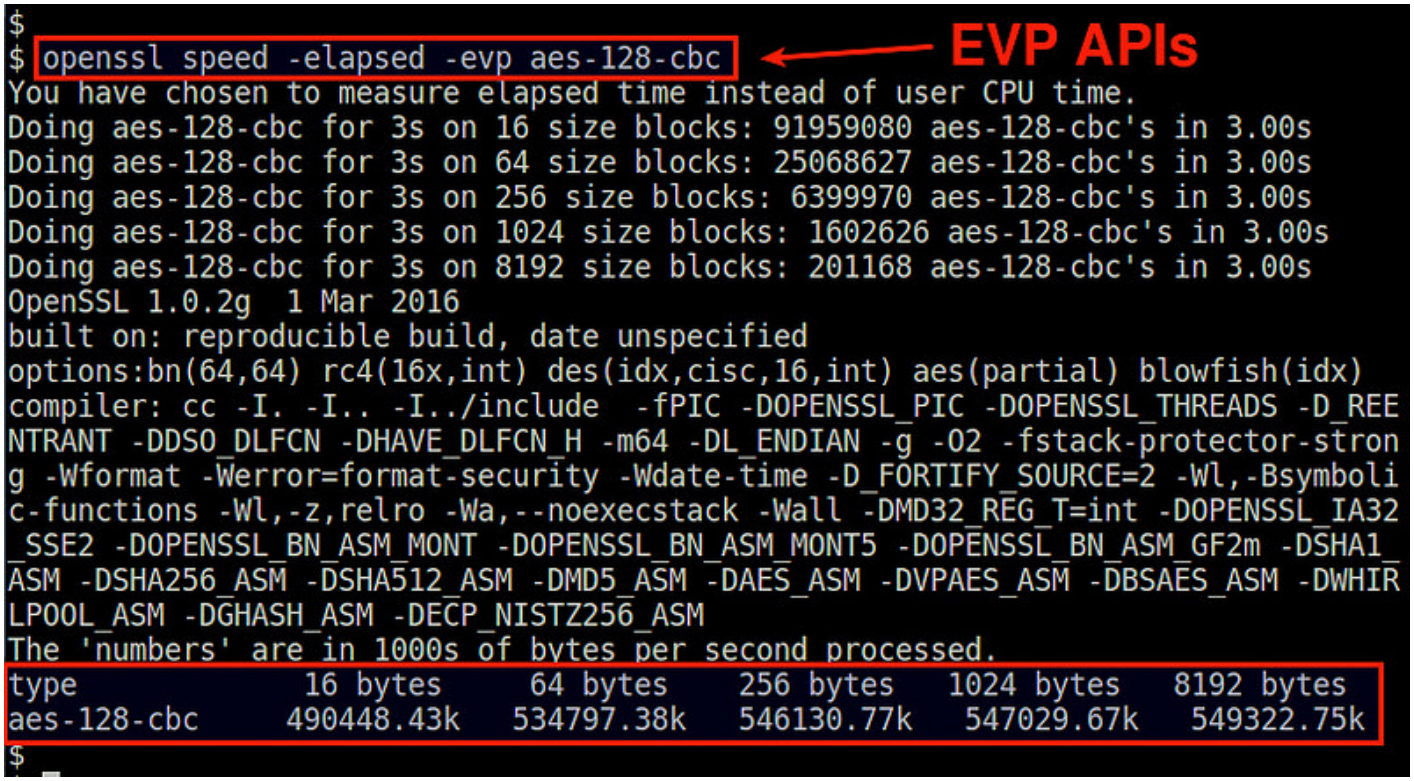
To measure AES algorithm speed without AES-NI acceleration:

```
$ openssl speed -elapsed aes-128-cbc
```



To measure AES algorithm speed with AES-NI acceleration (via EVP APIs):

```
$ openssl speed -elapsed -evp aes-128-cbc
```



The above two example outputs show encryption rates for different block sizes. You can see that AES speed with AES-NI acceleration is about five times higher than non-acceleration. This confirms that AES-NI is enabled for OpenSSL. If OpenSSL cannot leverage AES-NI for any reason, two outputs would show the same performance.