New instructions in Intel's advanced encryption standard (AES-NI)

In this article we will show you the importance of encryption and go deep into Intel AES-NI research.

In this article, I will show you the importance of encryption and go into Intel AES-NI.

With the growing popularity of computing devices in all areas, whether at work or at home for each of us, the need for encryption is becoming more and more important. now. Desktops, laptops, smartphones, 'pad' PCs, PDAs, Blue-ray players and many more, all need this need to be able to encrypt sensitive information. Without encryption, everything you send over the network (or even stored on an internal storage device) is potentially at risk, anyone can read it whenever they want. Whether authorization or access control can provide some form of protection, but when really interested in security, encryption must definitely be an important part of your multi-layer security campaign. . You might think that you have nothing to hide, but to know the truth, the information you think will be of no value to anyone can be taken advantage of in surprising ways. So, especially in today's corporate world, encryption needs to be taken seriously, not an optional one.

The importance of encryption

Scenarios where encryption will be used in our daily lives:

- When you turn on your laptop and automatically connect to your wireless access point, you will definitely use WPA encryption and AES encryption algorithms.
- When connecting to secure websites to share information or buy products online, SSL connections are an encrypted session designed to secure your personal information so that they are not shared with the the rest of the world.
- When a laptop uses BitLocker to encrypt the information on the disk, if it is lost, all of that information will not be public.
- When setting up an IPsec VPN connection or a DirectAccess connection based on IPsec for the corporate network, the IPsec connection will be secured with AES encryption.

There are many other examples, but it is clear that encryption and especially AES encryption is an integral part of our digital life, whether you know it or not.

As a network administrator, you probably know that encryption is an important part of your back-end architecture. Hackers will not care about knocking down your entire network the same way they did with previous exploits. Why? It is because there will be no money generated for wide area network attacks. With more and more penalties for criminal forms, most attackers are not doing this for entertainment purposes, but instead they are often an illegal business owner, wanting to earn Unrighteous money. One way they can do this is to compromise the main servers and silently break into it. Then steal salable information, such as your company's personal database or your company's trade secrets. Hackers often don't get anything with a "dead" server, and they can't get anything if you find out and block it before they get what he wants. As such, you need to use encryption on the back end as a protection mechanism in the 'last resort' to prevent an attacker from gaining access to important information.

Encryption is also part of everyday IT compliance; For example, all of the following are considered coding as part of their standards:

- HIPAA (Health Insurance Portability and Accountability Act)
- SOX (Sarbanes-Oxley)
- PCI DSS (Payment Card Industry Data Security Standard)

AES: A new standard

AES is an existing US government encryption standard and is used to replace the previous standard, triple DES, standard used a 56-bit key. AES also uses different key lengths, characterized by AES-128, AES-192 and AES-256. Depending on the length of the key, up to 14 transformations are required to create a final encrypted text.

AES also has several modes of operation, including:

- electronic codebook (ECB)
- cipher block chaining (CBC)
- counter (CTR)
- cipher feedback (CFB)
- Feedback output (OFB)

Cipher block chaining is the most used mode because it provides an acceptable level of security and is not likely to be vulnerable to statistical attacks.

Challenge between security and performance

The biggest problem with advanced encryption methods such as AES and CBC is that they require high processing power. Especially with the case of servers, but it can also be a problem for busy client systems, because on them are often installed inferior processors. That means you need to make your choice between getting the best level of security and getting the best performance for your systems. This situation can become difficult to resolve on the server side where solutions such as SSL or IPsec offload card (encryption offload card) are used to cool the processor and allow the processor. do tasks outside of session settings and bulk encryption.

The problem with add-on tags is, they are a standalone application and can or cannot work, depending on what you want to use them for. What we really need here is a general solution that can work in all AES encryption scenarios, the goal is for you not to have to do anything special to offload word encoding work. main processor. What we need is a 'plug and play' solution built into the operating system and motherboard.

Solve the problem with Intel AES-NI

If you agree with what we mentioned above, there are some good news for you - the new Intel AES-NI instruction set, included in Intel's Xeon5600 series processors, meeting these standards. This processor was previously known by the code name Westmere-EP. AES-NI implements a number of AES steps in hardware, right on the processor chip. However, you should know that AES-NI on the processor does not include the entire AES application but only some of its components, which are some components required to optimize performance. encryption rate. AES-NI does this by adding 6 new AES instructions: four for encoding / decoding, one for the 'mix' column and one for the 'next round' text creation (where the number of rounds is controlled by the bit length you choose).

One interesting thing about Intel AES-NI is that, because it is hardware-based, there is no need for the search tables inside the memory and the encryption blocks are executed in the processor. This reduces the chance of successful "side channel attack". In addition, Intel AES-NI allows the system to implement longer key lengths, and the end result gives us more secure data.

At this time, Intel AES-NI currently focuses on three main use cases:

- Trade securely over the Internet and intranet
- Full disk encryption (such as the feature provided by Microsoft BitLocker)
- Application-level encryption (part of secure transactions)

Secure transactions over the Internet and the intranet may include the use of SSL to connect to a secure website on the Internet or the intranet. In addition, IPsec transmission and tunneling modes are becoming popular for securing sessions over the intranet, and in the case of DirectAccess, over the Internet. It should be noted that SSL is used for layer 7 communications encryption, while IPsec is used to secure network level communication (layer 3).

Surely we've heard 'cloud' will be a big problem in computing, and cloud service providers will benefit from Intel AES-NI, where most of their communications are done via an encrypted channel. For IPsec, if there are only a few IPsec connections with one server, SSL offload may be good enough. However, if you have a busy

server, Intel AES-NI alone or in combination with SSL offload will be a better solution.

After obtaining the trading component of 'safe transactions'. In addition to application or network level encryption, there is an application-level encryption that can benefit from Intel AES-NI. For example:

- Database can be encrypted
- Email can be encrypted
- Rights management services using encryption
- The file system itself can be encrypted (as opposed to disk-level encryption).
- Applications such as Microsoft SQL can use Transparent Data Encryption (TDE) to automatically encrypt the entries created in the database.

It can be said that Intel AES-NI can significantly speed up transaction time and make customers feel happier, employees have better productivity.

Full disk encryption will perform encryption for the entire external disk from the MBR. In addition to Microsoft BitLocker, there are other disk encryption applications that can benefit from Intel AES-NI, such as PGPdisk. The problem with full disk encryption is that it can affect performance, which can prevent users from using it. However, with Intel AES-NI, that performance effect is basically unavailable, users will be able to enable full disk encryption and benefit from it.

Performance improvements

So what kind of performance improvements are there with Intel AES-NI? It's hard to say at this point because the technology is still so new. However, Intel did some tests and what they have received so far is quite good:

- With a bank-related amount of work using Microsoft IIS / PHP, they found that when comparing two Nehalem-based systems, one with encryption and the other one, the result increased by 23%. Users can be supported on the system. An encrypted Nehalem system compared to non-Nehalem systems, has improved 4.5 times as a number of supported users. It is an incredible number!
- In a test of Oracle 11g encryption and decryption, they discovered that, when comparing two Nehalem systems, one is encrypted and one is disabled, the system results are encrypted for found a reduction of 89% of the time to decode a 5.1 million encoding. It also reduced 87% of the time coding an OLTP table and repeated insertion and truncated one million rows.
- Full disk encryption consumes time for initial encryption. Intel found that, when encrypting an Intel 32 GB SDD drive for the first time using McAfee's endpoint encryption for PCs, the results showed a 42% reduction in time compared to the first attempt. It is a clear difference that you may have seen if you ever waited to complete an entire disk encryption process.

Conclude

Encryption is now a requirement in everyone's daily computing life. AES is a new standard for this issue. While encryption allows us to secure our data, there may be a significant performance cost associated with encryption and sometimes the overhead of encryption can take up some processor cycles from public What we want to do is done. In the past you could handle this problem by upgrading to more powerful processors, or adding more processors, or using offload encryption solutions. However, all of these methods have limitations. The new Intel AES-NI significantly improves performance and security by placing new AES-related instructions on the chip. This allows for increased performance and security for some scenarios, such as secure networks and application layer sessions, secure transactions, and full disk encryption with little or no affects the entire processor. Intel

AES-NI should be part of any client and server deployment plan, where encryption will be used on an extended basis, such as when DirectAccess is used to connect to the network. company. The combination of Nehalem and Intel AES-NI architecture promises a revolution in computing and improved governance satisfaction while improving performance.

For more information about Intel's Xeon 5600 series processors with Intel AES-NI, please refer here.