Making USB Flash drives secure: Why and How

By Anant Jhawar, Product Marketing Manager, Cypress Semiconductor Corp.

The USB based memory devices referred to as USB flash drive or “thumb drive” or “pen drive” have indeed revolutionized the way data storage and portability have evolved. Since their inception in 2000, millions of these devices have been manufactured and sold in all corners of the globe. Statistically speaking, approximately 173 Million units* of such USB based flash drives were manufactured in the year 2008 alone.

Some of the reasons which have contributed to the ubiquitous presence of these devices are:

- Portability: The physical form factor of these devices are generally quite small and light, making them very convenient for carrying around in one’s pocket (hence the name ‘pen drives!’)
- Ease of use: With the gaining acceptance of USB as a standard interface, these USB based storage devices are extremely simple to use. Just a simple plug-and-play is all it takes to use them!
- Low price
- Fast speeds
- Big (and growing) capacities

Of late, one of the major challenges facing individuals as well as corporations regarding the USB flash drives is that of data leakage and theft from these devices. There have been a number of cases ranging from misplaced to stolen or misused flash drives reported which have resulted in losses up to 2.5 Million USD* from a single such incident!

The losses are a result of confidential, personal or corporate level data getting leaked and misused. In the light of such occurrences, there is a need to make the USB based flash devices more secure and ‘leak proof.’ Data security can be maintained in USB flash drives using encryption/decryption mechanisms to enable reading/writing to the device only by authenticated personnel.

Security in USB flash drives

The two widely used methods for securing USB flash drives are:

1. Software encryption: Encryption keys are stored in the device’s memory and used to encrypt/decrypt the data. Although quite a safe methodology, the presence of the keys on the device memory exposes them to the hackers who know where to look for the keys and their unique format.
2. Hardware encryption: The encryption keys do not ever leave the hardware device, thus never exposing them. This aspect makes hardware encryption potentially more foolproof than the software encryption alternative.

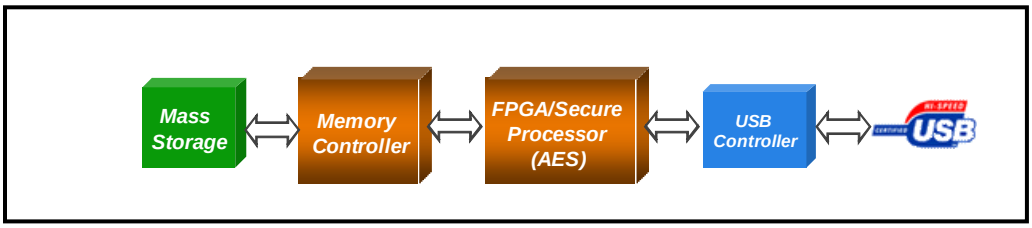
Both software and hardware encryption methodologies use the Advanced Encryption Standard (AES) 128-bit or 256-bit (As of now, neither the 128-bit nor the 256-bit algorithms have been reportedly compromised). However, just deploying the AES algorithm does not suffice as the manner in which it is executed is equally important. As is with software encryption, user-passwords are fed into the AES engine to generate the encryption keys, which makes the strength of the encryption directly dependant on the strength of the password. Also, ideally a 128-bit AES would require the password to be of 16 characters (8 bits/character) and similarly, the 256-bit AES would require a 32-character password. Creating and remembering a difficult-to-guess password can make the device user-unfriendly.

On the other hand, hardware based random number generators could be used to generate number patterns which would be fed to the AES engine to generate encryption keys. The encryption key is unlocked by the user password and is used by the AES engine for encrypting the data. Evidently, the hardware based methodology is a more secure option.

A point worth noting is that both the software and the hardware encryption methodologies require a user password. However, the hardware encryption method is deemed to be more fool-proof since it does not allow a direct access to the encryption keys and the quality of encryption is not determined by the strength of the user password.

A generic block diagram of such encryption enabled devices available today look like the following:

Published in Embedded.com (http://www.embedded.com/design/225402174) June 2010



In the schematic above, the USB controller receives data from the PC/laptop's USB port and passes it onto the AES engine which subsequently passes the data onto the mass storage in the encrypted format. The data retrieval also follows the same path in which the memory controller reads from the mass storage and passes the data onto the AES engine which decrypts the data and pushes it out to the USB controller.

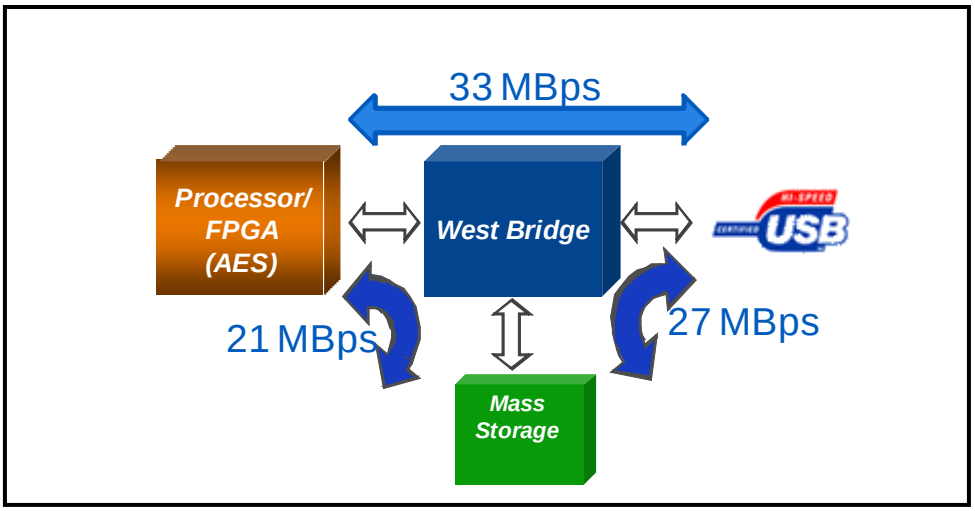
West Bridge approach

In 2006, Cypress Semiconductor introduced the West Bridge family of products. Similar to the North Bridge and South Bridge architectures in the PC world, West Bridge was introduced to allow evolution of embedded processors, independent from having to keeping up to speed with the changing memory and peripheral interfaces.

Effectively, a West Bridge device is a three-way bridge which offloads the processor from data intensive operations such as USB and memory management. The West Bridge device has three ports: one for connecting to the processor, one for connecting to the mass storage (two mass storage devices) and the third for connecting to USB for an external interface. The architecture of the device allows it to maintain three simultaneously bidirectional paths between the processor and the mass storage, the mass storage and USB, and the processor and USB. A marked advantage consequently is very fast data transfer rates between the ports.

The fast data transfer speed offsets the reduction in performance which can generally happen as a result of introduction of security features on the flash drive.

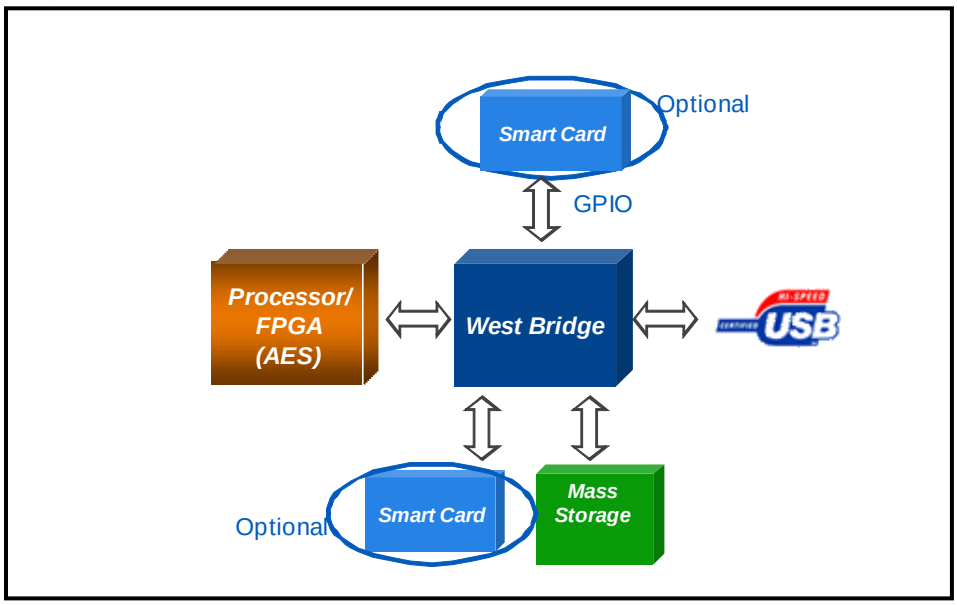
West Bridge can be used in the secure USB flash drive architecture as demonstrated below:



West Bridge completely controls USB handling and memory management in the architecture above. The processor/FPGA is offloaded from these tasks and handles only the AES encryption algorithm.

The data comes in through the USB port and is passed on to the AES engine which in turn sends the encrypted data to the mass storage. During data retrieval from the mass storage, the data is passed from the storage onto the AES engine which decrypts it and then passes it to the USB port.

Additionally, the same architecture can be scaled up as well as shown below:



Here, smart cards or other hardware equivalents are used to generate the encryption keys for the AES algorithm. A user password is required to unlock the encryption keys for it to be used by the AES engine for scrambling/descrambling the data. Scalability is an important feature as it allows for the OEMs/manufacturers to offer different versions of the device based on the same architecture.

Conclusion

With the wide scale adoption of USB as a connectivity standard on PC/laptops, and the evident advantages of the USB flash drives, it seems very probable that the USB thumb drives will continue to be the preferred storage media amongst consumers. However, the imminent risks discussed above emanating from the usage of this media also means that concrete steps have to be taken by manufacturers and OEMs in order to ensure safety of the data stored on the flash drives. A West Bridge based architecture can be used to address this concern, bringing along with it advantages like fast performance, BOM (Bill of Materials) cost reductions and use of a single-chip, scalable bridge solution.

Cypress Semiconductor
198 Champion Court
San Jose, CA 95134-1709
Phone: 408-943-2600
Fax: 408-943-4730
http://www.cypress.com