CONNECTINGINDUSTRY.COM

Electronics

NOVEMBER 2011

PRODUCTS AND APPLICATIONS FOR ELECTRONICS DESIGN

FUJITSU

MCUs tailored for control panels always at your fingertips

SENSING TECHNOLOGY

A sense for the tried and tested

Always at your fingertips

RACKS, CABINETS & ENCLOSURES: Staying cool under lock and key

USB data security: A problem solved

Danny Bradbury, Freelance Author for **Enova**, investigates how building encryption technology directly into USB protocol stacks at a hardware level can drastically mitigate data loss and compliance issues

Data security for removable storage may soon be a non-issue for many sensitive government and private sector organisations. The data loss and theft problem, which has proven to be an embarrassing compliance issue for many, can be stopped by building encryption and decryption technology directly into the controller hardware.

USB-based storage may offer the ultimate in convenience, but it is also becoming an unignorable security risk. In July 2011 the Ponemon Institute, which researches data breaches and security readiness among corporations, published a study highlighting the level of data loss from lost or stolen USB drives.

In the past two years, it discovered that 70 percent of companies traced the loss of sensitive business information to portable USB flash memory sticks.

Just over a third of businesses react by simply locking down all of their USB ports, so that USB storage cannot be used with their machines. However, this negates the benefits of USB storage entirely.

USB key flash drives are often seen as the biggest problem when it comes to USB-based storage, but they represent only a fraction of the removable storage market.

Furthermore, almost 80 percent of the USB-based hard drive products available today ship without security. The remainder often carry relatively weak security protection.

In response, ASIC design engineering company, Enova has released the 9th generation of its X-Wall DX chipset, designed to protect removable storage devices by factoring high-grade encryption directly into the hardware.

Previous generations of the chipset focused on other storage connectivity protocols. Originally, it provided an IDE-only interface, before upgrading to Ultra DMA mode 46. In subsequent generations, it migrated to SATA interfaces to support drives with serial interface faster performance, and then integrated USB and SATA interfaces on the same chipset.

Version 9 is the first generation of the chipset to include direct USB-to-USB communication, enabling it to support USB drives directly.

The X-Wall DX chipset protects removable storage devices by factoring high-grade encryption directly into the hardware

The chipset can be implemented in a variety of ways. PC or tablet computing manufacturers can choose to include it directly on one of the host ports, encrypting anything that passes across it. Alternatively, it can be built into the USB stack on the storage device, enabling a USB hard drive or flash drive to offer on-board encryption.

The third alternative is to put it on a hardware dongle designed to sit between the host port and the storage device. This dongle, which would have one simple USB in port and out port, would effectively become a physical key used to encrypt any USB storage media.

The chipset solves one of the biggest problems with conventional storage encryption, which is that authentication generally happens entirely on the host device. When host-based software is used to encrypt and decrypt data, it lays the user open to the risk of compromise. If an attacker can install malware on the host device and control the encryption software, they can compromise the secured data.

But by using both host and device-based authentication software, which is installed on the host device, and which the user uses to enter their personal identification number (PIN), the software then looks for the chipset for device-level authentication, providing a level of hardware-based protection that stops any malware from tampering with the system.

There are two levels of authentication with the chipset: user, and administrative. The administrative account is used to set the PIN for provision of the drive such as partition split, PIN and can also set parameters such as the number of failed attempts allowed. The user account is used to access the encrypted data.

The chipset allows for several different types of partitions on USB-attached storage. A cipher partition is hardware AES encrypted using the AES encryption protocol at the strength of up to 256 bits. The cipher partition is invisible and inaccessible until the user enters their PIN.

A public disk partition stores public data as a normal, unencrypted disk drive. There is also a read-only partition, and an optional write protect feature that prevents any data at all being written to the USB-attached storage device. This is particularly useful for preventing the writing of malware-infected files to USB storage, which could otherwise be unwittingly introduced to a corporate network.

Further protection is provided by the use of a logout feature, that allows the user to leave the computer for a break without needing to disconnect the drive. The data remains encrypted for that period, and cannot be accessed.

The encryption mechanism uses either Electronic Code Book or Cipher Block Chaining encryption.

Cipher Block Chaining uses an initialisation vector (IV) that performs an XOR function on each block of plaintext with the previous ciphertext block before being encrypted. This causes each ciphertext block to be dependent on all plaintext block processed up to that point.

It also uses an initialisation vector in the first block that is encrypted. All of this leads to an extremely strong encryption mechanism in which all blocks of data are protected, even if one encrypted block is broken.

In the past, this technology has been difficult to implement in real-time, making it unsuitable for encryption and decryption during data transfer.

The chipset is aimed at industries with particular needs for trusted mobile storage.

One sector that will find the system especially useful is healthcare. A doctor who wants to exchange a patient MRI data on a USB drive needs to do so securely, so as not to contravene the patient privacy provisions in the US HIPAA and HITECH Acts.

Using hardware-based encryption in real time helps to minimise the risk of data loss — and is an effective tool for IT departments wanting to remain compliant with security regulations, while offering their users the flexibility of removable storage.

Enova Technology
www.enovatech.net **Enter 235**