Safeguarding Your Data with Hitachi Bulk Data Encryption

HITACHI
Inspire the Next

Larry Swezey, Director, Mobile HDD Product Strategy and Marketing
Jim Wong, Software and Security Product Planning
Richard New, Research Manager

The growth in use of notebook computers as business machines has lead to an increase in the number of professionals carrying private customer data during their travels. It comes as no surprise that this trend leads naturally to an increase in laptop theft. Pound for pound, a laptop computer is one of the best targets for thieves—easy to carry, easy to sell. And, if the thief is lucky, access to private data that can be used for identity theft. Desktop PCs are being targeted for thefts from locked offices and homes as well.

Personal computers currently have four levels of security that can be utilized to protect content. These are listed below in order of what many consider "easiest to crack" to "hardest to crack."

1) Operating system-based system password
2) BIOS password
3) Hard disk drive (HDD) ATA password
4) Data encryption through either HDD hardware or system software

The OS-based password works when the system is up and running to prevent people from using the computer. It is effective for an office environment where a user would like to prevent others from using—and potentially changing—his computer without permission, or gaining access to confidential and personal data. However, in the case where a computer has been stolen, it is easy for someone to gain access to all the content on the system by simply removing the HDD from the system and inserting it into another machine or booting from a Linux CD.

The BIOS password is set in the system BIOS, resident on the personal computer's motherboard. It is more effective than the OS-based password because a user has to enter the password to even start up the system. However, there appear to be utilities on the Internet that claim to permit a user to overcome a BIOS password. Furthermore, as in the previous case, if a thief removes the hard drive and plugs it into another system without a BIOS password, the thief can easily gain access to the sensitive contents of the drive.

The HDD itself may also have a password, whose behavior is defined by the ATA security feature set. If enabled, the drive cannot be used without this password. In most personal computers, this represents the strongest security method available. A search of the Internet, including some forums where people routinely discuss how to defeat security schemes, reveals information that HDD passwords are very tough to crack. However, there are two potential weaknesses. First, a skilled technician could develop a custom tool to swap the electronics cards on the fly from two HDDs—one password protected, the other not—after startup in order to potentially defeat the password. Second, a person determined to read the contents of the hard drive could pay a data recovery service to physically dismantle the hard drive and then attempt to directly read all of the data from the disks using commercially available tools.

These examples of circumventing security are a bit extreme. It is reasonable to assume that most computer thefts occur with resale of the system as the primary motivation. However, systems providers who support major financial institutions, for example, cannot afford to take this level of risk. If a thief knew that there was a strong likelihood of gaining access to thousands of credit card numbers and social security numbers by paying someone to recover data from a stolen HDD, then the return in selling that information could be enough motivation for the thief to take that step. Furthermore, security and identity theft issues have been the subject of legislation, thus showing a recognition of the importance of protecting sensitive and important data. In the US for example, California enacted The Information Practices Act that relates to the security and confidentiality of personal information, see California Civil Code § 1798 et seq. With specific laws addressing data security, companies are likely to evaluate their security measures for protecting data.

A useful and strong solution for providing data security is encryption of the data on the disk , either by use of software or hardware. In other words, if the data on

the disk drive is scrambled in a way that cannot be understood without the decoding key, then even if a thief were to pay a data recovery service to recover the actual data on the disk drive, the data would be nothing but meaningless characters.

Data encryption is already possible through use of specialized software on the system. The software uses the power of the CPU to encrypt the data that is sent to the HDD, and then decode it when it is read back. This provides the added security, but with three key drawbacks. First is the cost of the software. Second, it requires CPU time to actually perform the encryption and decryption, forcing the user to accept a decrease in system performance for the added security and, in the case of a mobile laptop, reduced battery life. Finally, software security is more susceptible to attack than encryption implemented on a hard disk drive.

Hard Drive "Bulk Data Encryption"

It would be more advantageous to have the security of encryption without paying for extra software and/or losing system performance. A hard disk drive, with encryption as part of the HDD hardware itself, is such a solution. Bulk Data Encryption (BDE) by Hitachi enables a powerful encryption engine, Advanced Encryption Standard (AES), as part of the drive electronics System on Chip (SoC). When this option is enabled, the hard drive will encrypt all data that comes from the system and write it to the media. When read back, the drive decrypts the data so that it can be understood by the system. Since the hard drive is doing all the encryption work using hardware, there is no impact on system performance and no need for additional software. The AES-128 implementation in Hitachi BDE has received Federal Information Processing Standard (FIPS) 197 certification from National Institutes of Standards and Technology (NIST) (see http://csrc.nist.gov/groups/STM/cavp/documents/aes/aesval.html).

A Hitachi hard drive with the BDE option enabled is always automatically encrypting data, so the system user never has to worry about whether or not the data is being protected. Once the HDD password is set, the resulting security system on the disk drive is highly effective and difficult to penetrate. Furthermore, the drive encryption engine uses a 128-bit key. This means that the generated code would be very difficult to decrypt, even with the assistance of powerful computers and tools. For an idea of just how powerful this engine is, please refer to: http://www.nist.gov/public_affairs/releases/aesq&a.htm.

The implications for end users are huge. Once the HDD password is set, the user's data is continuously protected. One can easily imagine that HDD-based encryption would be highly attractive for any company routinely carrying sensitive information on laptops, desktops and SMB servers. Even if a system were lost or stolen, the company—and its customers—could rest assured that the data would have protection.

There is another note-worthy benefit that BDE provides. Currently, data on hard drives is relatively difficult to erase. To re-use a computer system, the hard drive must be overwritten many times to be sure that the previous data is erased. This is a time-consuming process. If a Hitachi drive with encryption is used, then simply erasing the key that serves as the basis for the encryption can instantly render all the data on the disk unrecognizable. If the hard drive is used again, then a new key is generated, and new data will be written over the old, unreadable data. "Enhanced Secure Erase," as it is called, saves a great deal of time and protects old and sensitive information from being inadvertently accessed. These two factors are likely to be of tremendous interest to companies who previously had to take extreme care and effort to erase old data on hard drives.

Hitachi offers the BDE option on all new 2.5-inch SATA hard disk drive products beginning with those launched in 2007, including both the 7200 RPM and 5400 RPM product lines. Hitachi also offers the BDE option on Deskstar products introduced in 2008 and beyond. For more information on how to use the encryption feature, see the "How To Guide" for Bulk Data Encryption Technology available on our website. Please contact your Hitachi sales representative for ordering information.

Hitachi Global Storage Technologies
3403 Yerba Buena Road
San Jose, CA 95135 USA

Produced in the United States 11/07. Revised 7/08.