

WHITEPAPER

Simplifying the complexities of encryption for business



Mobile users need to protect their personal information from identity theft. Businesses are mandated by federal and state law to secure personal information stored in electronic format.

Securing mobile storage devices has become a primary concern for most companies. One such concern involves the implication of losing a portable hard drive containing sensitive or personal customer information. Compliance legislation like Sarbanes-Oxley, HIPAA (Health Insurance Portability and Accountability Act) and other state legislation of personal information mandates the security of mobile devices must be considered when developing compliance strategies.

Compliance and portable drives

California's SB 1386 mandates the notification of California residents in the event of unauthorized acquisition of their "personal information" that is stored in an electronic format. Personal information includes the first and last name and either a social security number; drivers license number, account number, credit or debit card number, along with the security codes, passwords or access codes that would allow access to an individual's account. Fortunately, California's SB 1386 has made allowances when this sensitive data has been encrypted; this includes data on mobile devices

like the ThinkPad Secure HDD. If users are issued an ThinkPad Secure HDD for storing sensitive or personal customer data and the drive is lost or stolen, reporting the security breach is not required.

Compliance and networks

The exposure of personal information is not limited to portable devices. Corporate networks are also at risk of unauthorized access to this information. When a breach of security occurs, consumers will ultimately lose confidence, the company suffering damage to their reputation and financial losses. Enterprises are faced with a multitude of attacks and must make funding decisions on how best to increase their security infrastructure. Therefore, security products like the ThinkPad Secure HDD that protect access to and encrypt data on portable drive should be considered when making budget decisions.

Trademarks: Lenovo, ThinkPad and the Lenovo logo are trademarks or registered trademarks of Lenovo. Microsoft, Windows and Vista are registered trademarks of Microsoft Corporation. Other company, product and service names may be trademarks or service marks of others.

ThinkPad

© 2011 Lenovo. All rights reserved.

Visit Lenovo.com/safecomputing periodically for the latest information on safe and effective computing

Encryption

Types of Encryption

There are many types of encryption and many good resources with a complete explanation of the history of cryptography. This section examines why one type of encryption may be considered over another with respect to securing portable hard drives.

If the primary objective is to have a solution that is seamless, readily adopted by users and meet the mandated encryption requirements then 256 Advanced Encryption Standard (AES) is the best choice.

According to the Committee on National Security Systems (CNSS) Policy Number 15, Fact Sheet Number 1; "The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths."

As well, 256 AES is sufficient for all of local, national and International mandates for protection of personal information.

Hardware Encryption vs. Software Encryption

Software solutions for hard drives have been available for some time now. They have often been criticized for being inconvenient, slow and like any other software, prone to needing updates. Software encryption also ties up system resources and is vulnerable to key logging attacks.

In contrast, hardware encryption is very reliable, fast and convenient. Since hardware encrypted drives are not subject to updates, the costs related to traditional software solutions are eliminated. Immune to key logger attacks, a great advantage of hardware encrypted drives, they can also be easily reset. This reduces the amount of time spent scrubbing the drive or erasing disk data, which in turn stretches the IT department budgets when redeployment of assets is necessary.

Protecting Against Common Threats

The most common scenario involves an act of opportunity to use or resell the device after finding or stealing the hard drive. In this case the data would be completely protected regardless of the intended use. Using a hard drive with hardware encryption and restricted access, such as a user PIN would sufficiently protect the data stored on the drive from being accessed in the event of a stolen or found drive, even if the hard drive is removed from the enclosure. Without knowledge of the unique PIN, the drive could be redeployed by resetting the drive which erases the encryption key as well as all PINs and renders the data useless and inaccessible.

Cryptographic Attacks

The biggest concern for a user would be a theft targeting the data on the drive. Without knowledge of the PIN the thief may mount a cryptographic attack to unlock and access the data on the encrypted drive.

One approach may be to attempt to determine the encryption key used to encrypt the data. With the aid of a high speed computer and state of the art decryption tools, the thief might copy all of the raw encrypted data from the drive and attempt to decipher the encryption by trying different encryption keys until the encryption key was discovered. 128 bit AES offers a total of 3.4×10^{38} individual keys. It is estimated that if a DES key generator were able to discover 1 DES key per second, it would take 149 thousand-billion (149 trillion) years to crack a single 128 bit AES key. The likelihood of a successfully recovering the encryption key within several years is extremely unlikely. Only an extremely motivated thief with abundant resources and time would even consider this approach.

Another brute force attack might be to determine the PIN and would require a thief trying possible combination of keys to discover the correct PIN. The number of possible PINs based on a minimum length of 8 characters and a maximum of 16 would range from 8^{10} to 16^{10} for each PIN. Without knowledge of the PIN length the thief would have

to try all possible PIN lengths as well. Given the possible number of PIN combinations and built-in brute force protection a successful brute force attack via any method is extremely unlikely.

However, social engineering of the owner of the drive (to get the PIN) would be the easiest way to discover the PIN. This would involve an attacker deceiving the user into revealing the PIN or the attacker finds the PIN written somewhere. Also, an attacker could just observe the user entering the PIN as they access the device. Additionally, common PINs such as phone numbers, address, names, etc. would be considered by a motivated attacker. Electronic bugging of the target's home and office could also provide the PIN needed to access the device. Depending on the value of the data and motivation of the attacker, they may just choose to bypass the encrypted hard drive altogether and introduce malware into the target's PC as a way of acquiring sensitive data. There are many ways a motivated attacker may succeed against a targeted victim and many of them do not require a cryptographic attack.

Using Secure Password Policies

The device owner is the device administrator. He controls the PIN administration for the device for the administrator PIN as well as other users of the device. In a corporate environment, it is the owner's responsibility to follow company protocols for handling password administration including password length and password storage. However, all of the PINs

stored on the device will be completely protected and may only be deleted or replaced with a new PIN if the PIN is lost or forgotten.

For personal use it is important to follow some best practices when it comes to passwords.

- Don't share your PIN
- Exercise caution when entering your PIN
- Change your PIN regularly
- Don't use common PINs – names / birthdates
- Save your PIN in secure place

Key Generation/Management

Figure 1 illustrates the block diagram of the construction of the ThinkPad Secure HDD. The encryption chip encrypts and decrypts the data based on a 256-bit AES key. This AES key is only accessible by the encryption chip and not accessible by the user. The user would need to login with the correct PIN, using the keypad, before the drive is unlocked and recognized by the host system. At this point the encryption chip begins the encrypting and decrypting operations allowing access to the hard drive.

The Lenovo ThinkPad Secure HDD handles authentication without sending any data to the computer. Once the correct PIN is entered in the keypad, the microcontroller allows access to the drive. Since the PIN is never sent to the computer, it is not possible for software on the computer to intercept the PIN, thereby protecting against key logging attempts.

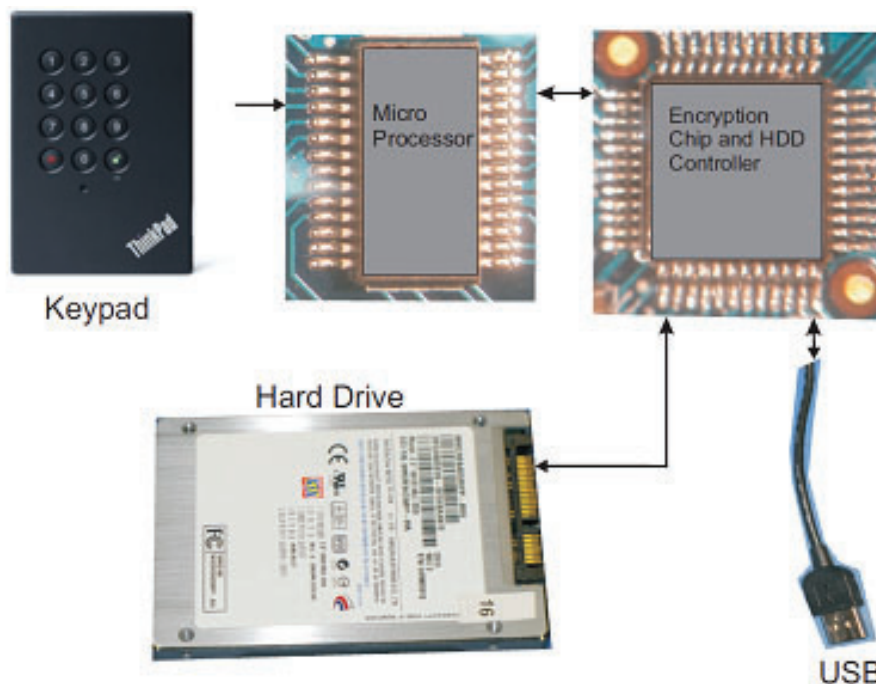


FIGURE 1

WHY CHOOSE THE
SECURITY OF

THINKPAD
SECURE HDD?



Lenovo ThinkPad Secure HDD

Lenovo's ThinkPad Secure HDD is the ultimate portable hard drive and secure storage system. The ThinkPad Secure HDD's unique design features include an easy-to-use keypad and software free design that enable access to the drive with a unique personal identification number (PIN, aka password) on virtually any USB equipped system and is compatible with virtually any operating system. Simply plug in the ThinkPad Secure HDD into any powered USB port, enter the secret PIN and access the encrypted data.

The ThinkPad Secure HDD incorporates a National Institute of Standards and Technology (NIST) certified 256-bit AES hardware encryption algorithm.

The ThinkPad Secure HDD includes a standard SATA 2.5" hard drive and is housed in an enclosure that includes the user interface, encryption circuitry, integrated USB cable and shock mounting for the hard drive. The ThinkPad Secure HDD is formatted with a single encrypted partition that provides seamless on-the-fly encryption for keeping data safe and protected even if the hard drive is removed from its enclosure. The ThinkPad Secure HDD supports up to ten users and one administrator each with a unique PIN with a minimum of 8 characters and a maximum of 16.

Target customer

The ThinkPad Secure HDD is designed for corporate, government and personal users whose data should be accessible only by the designated users or system administrator. Business users are mandated by federal and state laws to protect customer's personal information and the penalties can be very costly in actual fines as well as damage to the company's reputation as customers are notified about the breach.

No software installation is required for setup or operation, providing for a simplified deployment in corporate environments. The administrator feature allows enrollment of up to ten unique user ID's and one administrator, making it a useful business collaboration tool.

Most government agencies require users to store all information on at least AES 128 bit encrypted hard drives for information that is considered "secret level". Personal users need a safe harbor for personal data financial records and so forth.

All three types of users can now store confidential information in a password protected, hardware encrypted portable storage device with AES 256 bit encryption. Only upon a successful authentication will the information become accessible.

ThinkPad Secure HDD Hardware Encryption

The ThinkPad Secure HDD uses 256 bit AES real-time encryption with the Initio 3607 cryptographic engine which is NIST (National Institute of Standards and Technology) and CSE (Communications Security Establishment) hardware AES (Advanced Encryption Standard) certified algorithm, certificate number #1174.

Protection from Key loggers

The ThinkPad Secure HDD creates a secure “Trusted Path” between itself and host computer that protects all data on the drive. An additional security feature includes the way the ThinkPad Secure HDD is recognized by the operating system. Once the USB cable is connected, the operating system sees the ThinkPad Secure HDD as a removable device in ‘media not present’ state, so accessing the drive is not even possible.

As the ThinkPad Secure HDD does not employ software and requires the PIN to be entered via the onboard keypad before being it can be accessed, key loggers do not have the opportunity to capture your password inputted via a keyboard. After PIN login is completed the device is unlocked and the operating system invokes a ‘media inserted’ event.

Complete security is ensured with the data stored in AES encryption; even if the drive is removed the data will be completely inaccessible.

Protection against Brute Force Attacks

The ThinkPad Secure HDD is designed to allow 5 PIN attempts before blocking additional attempts. Once the ThinkPad Secure HDD shuts down the user will need to unplug the drive by removing power, then plug in the drive again. Once the total number of unsuccessful attempts reaches 25 the drive will lock and require a “special” PIN to allow another 25 attempts. When the total number of unsuccessful attempts reaches 50 the drive will lock and require a complete reset. The reset will also reset the encryption key making any data on the drive un accessible. Given the possible number of PIN combinations and built-in brute force protection a successful brute force attack on the ThinkPad Secure HDD via any method is extremely unlikely.

Why choose the ThinkPad Secure HDD?

1) Access to the ThinkPad Secure HDD is protected via a secure PIN.

The ThinkPad Secure HDD drive is only recognized by the host computer once unlocked by the user’s unique PIN. Up to ten different PINs can be used, making the ThinkPad Secure HDD a secure business collaboration tool.

2) The ThinkPad Secure HDD’s encrypted hard drive seamlessly encrypts data in real-time with 256 bit AES XTS encryption.

The data on the drive remains impenetrable, even if removed from its enclosure, ensuring the utmost in protection for even the most sensitive files.

3) Rugged and Compact.

Perfect for taking on the road, the ThinkPad Secure HDD’s compact design includes an integrated USB cable and shock mounted design.

Summary

The Lenovo ThinkPad Secure HDD is the ideal solution for corporate, government and personal users whose data should be accessible only by the designated users or system administrator. The ThinkPad Secure HDD’s low powered design is perfect for taking your data on the road. This ultimate secure hard drive features a compact robust design and a 16-point omni-directional shock mounting system, protecting the drive from drops and knocks. The convenient integrated USB cable eliminates the need to carry around cables and allows connection at the flick of a fingertip. Whether you need to protect highly sensitive corporate documents, personal information, trade secrets or customer data, the ThinkPad Secure HDD is the ideal hard drive to safely transport your data.

ThinkPad

© 2011 Lenovo. All rights reserved.

