Disk Encryption Using a Physical Key

WeiTi Liu
LucidPort Technology, Inc.
sales@lucidport.com

Background

- Increasing Need for Data Protection
  - Using software to block and monitor data breach activities are effective but most of the times are playing catch-up role.
    - http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/
- Survey shows many files/datum on computer disk, Flash drive, external hard disk and Cloud computing are not encrypted.
  - http://www.sfgate.com/business/article/Druva-Survey-Reveals-Enterprise-Laptops-More-2358205.php
  - http://www.technewsworld.com/story/5-Tips-for-Braving-the-BYOD-Boom-75326.html
- Existing Solutions
  - Require complex setup
  - Fixed on one computer or storage, nontransferable
  - Not easy to use
  - http://www.youtube.com/watch?v=QGslrUwUO8M
  - http://www.youtube.com/watch?v=JDaicPIgn9U

Existing Solutions

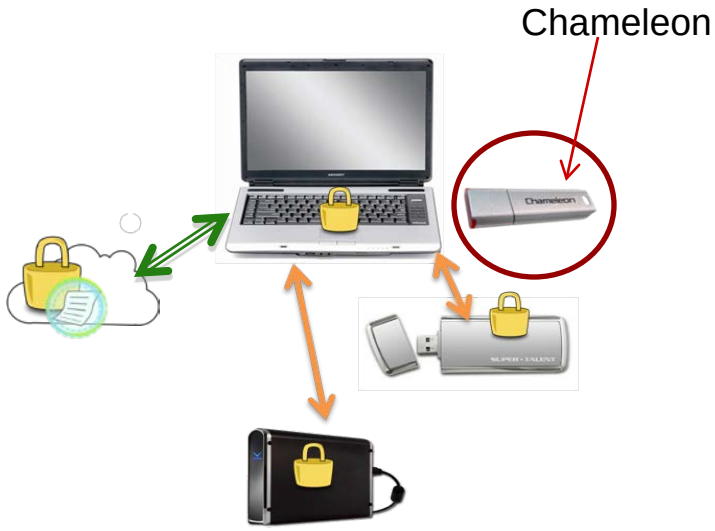
- Software encryption (TrueCrypt, BitLocker, etc.)
  - Since the PC must know the encryption key, it can be attacked by hackers, spyware, key-loggers, and other software (like Kon-Boot)
  - Vulnerable to cold boot attacks (recover encryption key from RAM)
  - Yet another password that can be stolen without your knowledge
- Encrypted disks/ Thumb drives
  - You lose your data if the disk is lost or broken
  - Your backups are unencrypted. Backups can only be made with the drive unlocked.
  - Traces of your private files remain in the PC's hard drive
  - Limited capacity
  - Yet another password that can be stolen without your knowledge

Hardware encryption (Chameleon, Encrypted Disks) versus Software encryption

	Software	Hardware : Encrypted Disks	Hardware : Chameleon (LucidPort)
Encryption Key Management	Complex	Drive provides single key	User controls encryption keys (easy and secure)
Costs	High: Continuing (upgrade) life cycle costs	Medium: Pro-rated into the initial drive cost	Low: Fixed at one time purchase cost
Migration or Re-Encryption	Complex	None	Easy
Installation and Use	Complex	None	Easy and secure
Supports multiple devices	Yes, new setup for each drive	Fixed, can only use for single drive	Supports multiple drives and devices

Objectives

- A general purpose data protection device with strong encryption can be used in anywhere,
  - o supporting multiple computers
  - o storage devices including external flash drive and hard disk
  - o Cloud computing
- Easy to use
- Secure

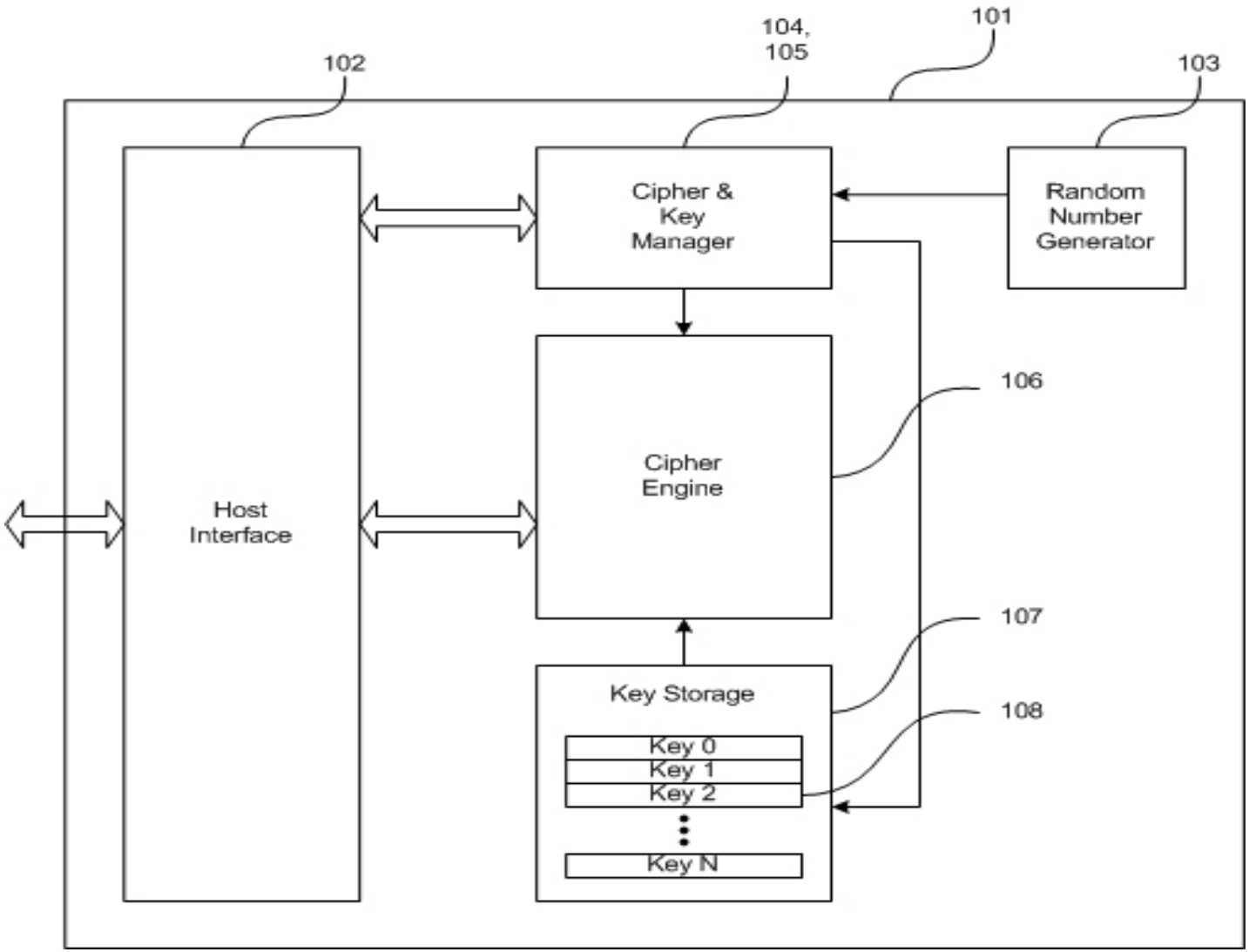


Dilemmas

"A secret known by two is no longer a secret"

- The actual encryption and decryption is performed by a program running in the computer.
  - a copy of the encryption key is present in the computer's RAM, in a place accessible to the program that is performing the encryption.
- An encryption scheme that relies on passwords.
  - vulnerable to several possible attacks including, key-logger software, surveillance

Chameleon Block Diagram



Architecture

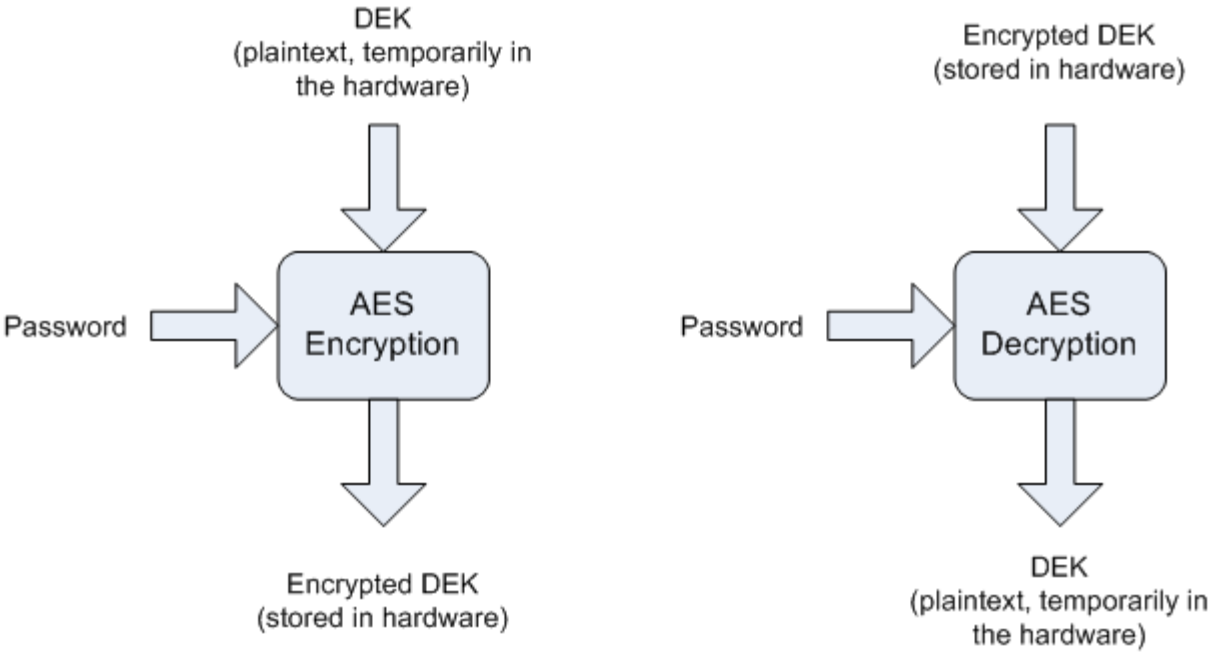
- Encryption and decryption is performed by the external device, not by the computer.
- Encrypted data is stored on the computer's hard drive, or on the external storage devices.
  - Flash Drive, External Drive (Hard Drive, SSD etc.)
  - Cloud Storage
- Passwords are not required.

Software

- An installer initializes the device and creates a file in the Chameleon directory.
  - A service makes this file look and act like a disk drive to the operating system. It intercepts all accesses to and from this drive.
  - These accesses are translated to commands for the Chameleon device.
  - A custom driver sends these commands and associated data to the Chameleon device, instructing it to encrypt or decrypt the data.
- The integration of these three parts creates a seamless experience for the user. The user accesses the encrypted partition/ drive (which is just a file). These accesses are intercepted and sent to the Chameleon device for encryption or decryption.

Password Protection

- DEK is stored in hardware in plaintext, when Password protection is enabled, an encrypted version of the DEK is stored in the hardware instead.



Authentication

- Password
  - Password for added security.
- Physical key
  - Convenience
- Recovery Passphrase
  - Secure
  - Only use during setup time or key backup time, no need to type Recovery Passphrase for normal usage

If you lose your User Chameleon

- Admin creates a duplicate User Chameleon
  - Insert the master Chameleon key.
  - Create a user key, enter the user ID, specify if a password is required
  - Unplug the master key then insert a user key
  - The user key will be programmed with the specified user ID

- Locking out the lost Chameleon
  - Insert the master Chameleon key into the PC with the Chameleon drive
  - Select “Change Encryption”
  - Assign a new user ID to the Chameleon drive
  - Chameleons with the old user ID can no longer access the drive
  - The old user keys can re-programmed with the new user ID

Applications

- Transfer and store sensitive information, such as bank account information, driver license numbers, social security numbers, employee records, customers, patient information or IP.
- Encrypt internal or external drives (Hard drives or USB Flash drives)
- Encrypt E-mail attachments
- Store data to cloud storage
- Store emails, web login links' passwords, such as, Social networks accounts(Facebook, Twitter, LinkdIn, YouTube)

Chameleon adds security for full Disk encryption drives

- Full disk encryption subjects,
  - Hackers attack
    - Kon-boot etc.
- Chameleon in computer with full disk encryption provides highest level security for computer (laptop or desk top).
  - Plug Chameleon key in your computer, you can access files in Chameleon drives and other drives.
  - Remove Chameleon, all files are protected in your Chameleon drives, Windows remains fully functional. Chameleon hides your files from Key-loggers, spyware, malware, trojans, and hackers.

Why Encrypt data on Flash Drives?

- Flash drives are easily lost or stolen
- Flash drive contains sensitive data

Source:
http://www.credant.com/campaigns/usb_survey/

Summary

- A new architecture of data protection device(Chameleon) is presented to address current solution's dilemmas
  - The Chameleon avoids the problems associated with passwords and software encryption.
- The Chameleon is designed for businesses, governments, and individuals who want to easily protect the data on their computers and external storage devices.
  - Chameleon is designed for data encryption not for disk back up
  - The Chameleon guards your data even if Windows is not password protected. Windows remains fully functional without the Chameleon plugged in.
- Like a physical key, you can replace keys, share keys, create a master key, make duplicates, or change the lock.

Contact

- Technical Support
  - o support@lucidport.com
- Sales/ Business Inquires
  - o sales@lucidport.com
- Address:
  - o 485 E. Evelyn Ave., Sunnyvale, CA 94086
- Tel: 408-720-8800, Fax 408-720-8900
- www.lucidport.com