Secure Storage Portfolio for Sale

Feisal Mosleh
SVP IP M&A

For Recipient Only
Do Not Forward without Permission

CryptaByte Portfolio for Sale

- 7383386 B1, 7876894 B2, 8230207 B2
- Examples of acceptance in the market:
  - IronKey, Bought by Imation is a licensee
  - IronClad is JV between IronKey and Lockheed Martin

- IronClad is a "PC on a stick" developed through a joint-venture between IronKey and Lockheed Martin
- IronClad houses an entire operating system, applications, and data on a USB flash drive—all of it protected by CryptaByte Hardward-Based Encryption technology
- IronClad was featured at the 13th Annual Congressional Internet Caucus Advisory Committee Kickoff Technology Policy Exhibition
- Lockheed Martin's award-winning IronClad technology is a secure, encrypted flash drive that lets employees carry their entire desktop – including the operating system, applications and files – on a rugged USB drive the size of a stick of gum
- IronClad is a fast and affordable way to stand up a telework program without issuing every employee a laptop or making a large investment in a virtual desktop infrastructure

Lockheed touts "PC on a Stick" for Feds

Posted January 21, 2011 - 11:15 by Trent Nouveau

Lockheed Martin has upgraded its IronClad USB drive with improved security features and optimized management tools.

Indeed, the federally approved IronClad allows employees to carry their entire desktop - including the OS, apps and files - on a rugged USB drive the size of a stick of gum.

"The latest release, version 1.8, is faster, works with a wider array of PCs and laptops, supports more Wi-Fi networks, and makes it easier for IT administrators to track, manage and even shut down the drives if need be," explained Lockheed spokesperson Rohan Amin.

"Federal employees can plug in their IronClad drives to their home computers and boot their entire work desktop. That makes them fully productive at home, and backed up by rock-solid security."

According to Amin, IronClad allows IT administrators to monitor and update every drive on their network.

"[So], if a drive is lost or stolen, new features give administrators more options for disabling the drive. The system's performance is also faster than ever, and new wireless features make it easier to connect securely to home Wi-Fi networks.

"With five layers of cyber security and tamper-resistance, IronClad will keep government networks and data secure while employees work in the office, at home or on the road," he added.

- The "Cryptochip" is a real-world implementation of CryptaByte hardware-based encryption, and is the foundation of IronKey's industry-leading data protection devices
- Awarded Best Mobile Device Security Solution by SC Magazine at RSA Conference 2008
- Stimulated Acquisition of IronKey by Imation, and has grown into a successful line of products

Overview

- Data security is paramount (and increasingly mandated), but enterprises are struggling against barriers of cost, reduced performance, and increased complexity.
  - Despite the regulations mandating encryption of sensitive data, many organizations have resisted encryption because the majority of solutions are complex, slow, software-based solutions
  - Concerns over software-based encryption have caused many organizations to look towards the growing number of hardware-based encryption solutions available
- The CryptaByte Portfolio's EnigmaCells™ technology provides a cost-effective and unbreakable hardware encryption method with **no impact on real-time performance**.
  - CryptaByte EnigmaCells™ technology protects critical information by encrypting the data using dedicated hardware, an unbreakable encryption key, and encrypting data memory block by memory block

Technology	Cost	Impact on System Performance	Data Vulnerability
Software Encryption	High	High	High
State-of-the-Art Hardware Encryption	Low	Low	Medium
CryptaByte EnigmaCells™	Low	Low	None

Technology and Applications

EnigmaCells™

Chips implementing CryptaByte Enigma Cells™ technology generate a unique encryption key sequence for each addressable block of memory; and by using a true random number generator, only a portion of the encryption key is stored in the device making it impossible to access the encryption key — thus providing superior protection for storage devices against brute force attacks and offline parallel attacks.

Advantage	EnigmaCells™
Cost	Prevents costs of data theft, not costly and complex to deploy
Performance	Hardware encryption is transparent to the end user, with no noticeable slowdown compared to software-based encryption
Reliability	CryptaByte partial random key generation is unbreakable

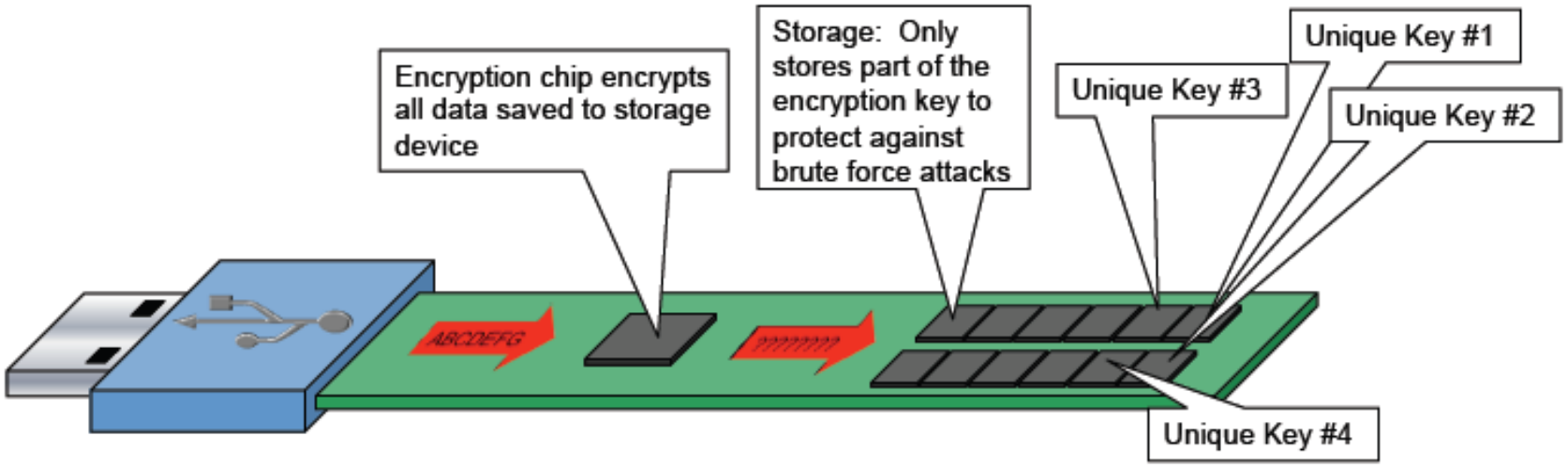
CryptaByte Technology

Features:

- EnigmaCells™ chip encrypts data stored on a storage device (e.g. USB flash media)
- Only stores a portion of the encryption key in the storage device and randomly generates the remaining sequence for unbreakable encryption
- Individual blocks of memory are assigned a unique encryption key sequence, ensuring the full volume of data is protected

Benefits:

- Provide superior protection for storage devices against brute force attacks and offline parallel attacks
- Memory block-level encryption ensures remaining blocks of memory stay encrypted—even if a single block's key is decrypted
- Easier to deploy, manage, and recover
- No system lag to end-user, as normally experienced with software-based encryption



US8230207 Summary

Patent: 8230207

Priority: Jan 30 2007

Filed: Sep 29 2010

Issued: Jul 24 2012

Expiry: Jan 30 2027

System and method of providing security to an external attachment device

Key Claims:

7. In a system comprising a computing device having a USB port and an external storage unit having a USB controller, a method comprising:on controller startup, the controller presenting to the computing device via the USB port data from a first partition of the external storage device as a Read Only Memory, whereby the computing device is caused to assign to the first partition a drive letter and provide to the first partition read access;

causing the execution of an authentication process; and

in response to receiving a valid authentication, the controller presenting to the computing device a second partition of the external storage device, wherein the second partition remaining invisible to the computing device until presented, and whereby after presentation the computing device is caused to assign to the second partition a drive letter and to provide to the first partition read/write access.

6. A system comprising:means, on controller startup, for the controller presenting to a computing device via the USB port data from a first partition of the external Serial Advanced Technology Attachment storage device, as a Read Only Memory, whereby the computing device is caused to assign to the first partition a drive letter and provide to the first partition read access;

means for downloading from said controller into said computing device and causing the execution in said computing device of an authentication process; and

means, in response to receiving a valid authentication, for presenting to the computing device a second partition of the external Serial Advanced Technology Attachment storage device as an eSata storage device, the second partition remaining invisible to the computing device until presented, and whereby after presentation the computing device is caused to assign to the second partition a drive letter and to provide to the first partition read/write access.

US7876894 Summary

Patent: 7876894

Priority: Nov 14 2006

Filed: Nov 14 2006

Issued: Jan 25 2011

Expiry: Aug 17 2029

Method and system to provide security implementation for storage devices

Key Claims:

12. A method comprising:for each set of consecutively addressable blocks of a storage device into which encrypted data is stored, a set comprising two or more consecutively addressable blocks, generating a multi-byte random number unique to that set from a random number generator, the random number generator comprising a hardware register whose value is unpredictable on power up;
generating an initialization vector from the random number, the initialization vector being independent of the data; encrypting data to be stored in a set employing the initialization vector as at least a portion of an encryption key; storing the random number in the set; and storing the encrypted data into the set.

1. A method comprising:for each addressable block of a storage device into which encrypted data is stored, generating a multi-byte random number unique to that block from a random number generator, the random number generator comprising a hardware register whose value is unpredictable on power up; generating an initialization vector from the random number, the initialization vector being completely independent of the data; encrypting data to be stored in a block employing the initialization vector as at least a portion of an encryption key; storing the random number in the block; and storing the encrypted data into the block; wherein the initialization vector depends on a random number stored with the data and is not dependent upon the data.

US7383386 B1 Summary

Publication number	US7383386 B1
Publication type	Grant
Application number	US 10/850,813
Publication date	Jun 3, 2008
Filing date	May 21, 2004
Priority date	May 21, 2004
Fee status	Paid
Also published as	US20080229005
Inventors	Sree Mambakkam Iyer, 3 More »
Original Assignee	Mcm Portfolio Llc
Export Citation	BiBTeX, EndNote, RefMan
Patent Citations (23), Referenced by (11), Classifications (12), Legal Events (6)	
External Links: USPTO, USPTO Assignment, Espacenet	

US 7383386 B1 Key Claims

- US 7383386 B1 - Multi partitioned storage device emulating dissimilar storage media
- Abstract: A digital media. In one embodiment, the digital media devices includes a storage unit/partition that emulates a Compact Disc-Read Only Memory (CD-ROM), and optionally, a second storage unit/partition that acts as a Read/Write storage device.
- Key claims:

1. An apparatus comprising:a connector to connect to a computing device;

a first storage partition having a Read Only Memory (ROM) storage unit;

a Read/Write storage unit comprising a card-reader for accepting a flash memory card, the flash memory card comprising a second storage partition;

firmware to emulate a CD-ROM using the ROM; and

a master boot record to identify at least two partitions of the apparatus including the ROM storage unit and the Read/Write storage unit.

11. A method comprising:accessing a master boot record to identify at least two partitions of the apparatus including a Read Only Memory (ROM) storage unit and a Read/Write storage unit;

providing a portion of a first storage partition from the ROM storage unit to a computing device;

providing a portion of a second storage partition from the Read/Write storage unit comprising a card-reader for accepting a flash memory card, the flash memory card comprising a second storage partition; and

emulating a CD-ROM using the ROM.

14. A machine-readable medium having stored thereon a set of instructions that when executed on a machine will cause the machine to perform a method comprising:accessing a master boot record to identify at least two partitions of the apparatus including a ROM storage unit and a Read/Write storage unit;

providing a portion of a first storage partition from the ROM storage unit to a computing device;

providing a portion of a second storage partition from the Read/Write storage unit comprising a card-reader for accepting a flash memory card, the flash memory card comprising a second storage partition; and

emulating a CD-ROM using the ROM.

Contact: Feisal Mosleh FMosleh@Kanzatec.com
650 468 0401
SVP IP M&A

For Recipient Only
Do Not Forward without Permission