IBM® Virtualization Engine TS7720 Series
Disk Encryption Overview Version 1.0

By: Felipe Barajas
IBM Advisory Engineer
Tucson, Arizona
Introduction

The IBM Virtualization Engine TS7720 Series is the latest in the line of tape virtualization products that has revolutionized the way mainframe customers utilize their tape resources. Security of the information stored on the internal disk subsystem used to virtualize tape has become important to many customers. The TS7720 internally uses a disk subsystem to store or cache virtual tape volumes. The IBM TS7720 disk subsystem model 3956-CS9 has been enhanced to support encryption in June 2012. This white paper describes the use of data encryption on these disk subsystems when used in the TS7720 Virtualization Engine (VE).

Summary of Changes

This is the initial version of this document.

Overview

The importance of data protection has become increasingly apparent with news reports of security breaches, loss and theft of personal and financial information, and government regulation. Encryption of the local disk subsystem internal to the TS7720 helps control the risks of unauthorized data access without excessive security management burden or subsystem performance issues.

The disk encryption solution for tape virtualization consists of several components. IBM’s disk encryption solution uses Full Disk Encryption (FDE) disk drives inside the 3956-CS9 and its expansion drawers (model 3956-XS9). These drives are Self-Encrypting Drives (SEDs).

These disk drives or Disk Drive Modules (DDMs) contain the cryptography chipset necessary to implement a hardware-based encryption solution. This solution is based on the AES-128bit encryption standard and adheres to the Trusted Computing Group (TCG) enterprise security requirements. Additionally, this solution complies with National Security Agency standards by implementing government-grade encryption.

This encryption solution minimizes management burden by locally managing the disk encryption implementation. Using local encryption management fully automates the encryption solution by not requiring external key servers or additional software to maintain.

Because disk drive modules routinely fail, disk encryption ensures the failed drive can be safely disposed of knowing that its contents are encrypted and thus unreadable.

Code Requirements

Disk encryption was introduced with the TS7720 Virtualization Engine microcode version 8.21.0.130 in June 2012. There are no additional host software updates required for the disk encryption function.
**Disk Encryption Introduction**

Disk encryption protects data at rest. The TS7720 uses multiple Redundant Array of Independent Disk (RAID) Drives in the internal disk subsystem to protect and store virtual tape volumes. This internal disk subsystem is the only subcomponent of the TS7720 that stores and contains the security sensitive virtual tape volumes. Virtual tape volume data and information is protected by encrypting the individual drives that form the RAID arrays. This solution therefore protects the data sensitive virtual tape volumes by encrypting the resting place of that data in the TS7720, i.e., the individual drives that form all RAID arrays in the subsystem. This solution complements other types of encryption solutions that may be available such as tape encryption or encryption of data while in transit.

The disk encryption is implemented by hardware inside each disk drive module. Each disk drive module (DDM) inside the TS7720 disk subsystem contains a cryptography chip that encrypts its own data. Using this hardware based approach ensures optimal performance. If one or more DDMs become exposed to unauthorized third parties the data contained within that drive will be unavailable and unreadable without the proper encryption key.

Encryption keys are locally managed. The encryption key is contained internally by the TS7720 in a non-volatile memory area that is only accessible by the internal disk subsystem controllers’ memory (non-volatile RAM). When this key is copied to areas outside this protected memory, the key is encrypted with its own algorithm in order to obfuscate and thus avoid being intercepted unknowingly. An obfuscated copy of this key is stored as a backup inside the 3957-VEB. This backup copy can only be accessed manually by higher levels of service personnel during disaster recovery scenarios, for example, in the rare event both disk controllers need to be replaced at once. At customer request, this obfuscated key can be optionally backed up to media outside the TS7720 (such as CD or DVD disks).

**Locally Managed Encryption Keys**

The encryption key does not play part in the actual encryption algorithm used by each disk drive module (DDM). The encryption key is not used to encrypt the data stored inside each DDM, rather, the key is used to unlock the DDM. Without the proper key, the drive will lockup and the drive will be unavailable for any type of I/O (read or write). This allows the key to be changed at any time without having to wait for the drive to re-encrypt itself. This is a double protection mechanism. With encryption enabled, every single DDM in the TS7720 will be physically encrypted and every single DDM will only do I/O if the correct key is provided.

The TS7720 provides a mechanism to enable, generate and change encryption keys. Encryption can be enabled on-demand and because the key can be changed independent of the physical disk encryption, customer downtime is minimized to virtually minutes instead of waiting for days for existing data to be encrypted. However, once encryption is enabled it cannot be disabled; this ensures permanent data protection.

**Prerequisites**

While the feature for disk encryption support is customer-installable, actual enablement may require configuration by an IBM Service representative.
TS7720 Virtualization Engine Microcode
The Virtualization Engine (VE) must be running microcode level 8.21.0.130 or higher. The disk encryption feature code must be installed to access the encryption settings.

TS7720 Virtualization Engine Hardware
The TS7720 Virtualization Engine (VE) must contain compatible hardware in order to enable disk encryption. This compatible hardware must include a disk subsystem populated with only FDE capable drives. TS7720 systems shipped before June 2012 may not contain this new hardware. TS7720 vital product data (VPD) can be analyzed by IBM service representatives to ensure existing hardware meets these requirements.

Installation
The disk encryption feature code provides explicit instructions on setting and enabling disk encryption. These illustrated instructions are not repeated in this paper. Briefly, the installation steps are:

- Customer installs the proper feature code using the Maintenance Interface (MI)
- IBM Service Representative enables encryption from the TS7720 VE service menu

Encryption is completely transparent to the operation of the TS7720. Once activated, encryption cannot be disabled. However, the encryption key can be re-generated at any time by IBM service representatives from the VE service menu.

Maintenance
There are no additional maintenance requirements with locally managed disk encryption. All disk drive modules (DDMs) that form the RAID arrays must be Full Drive Encryption (FDE) capable. When an FDE capable DDM fails, the TS7720 will automatically inform service personnel the replacement part number needed. This ensures a failed FDE drive is replaced with another FDE capable drive. Note that the system will not allow a non-FDE drive to be inserted once encryption is enabled. Due to the transparency of locally managed encryption, other TS7720 subcomponent upgrades, part replacements etc. are not affected and will continue to work the same way as systems without disk encryption enabled.
Local Disk Encryption Internals

RAID Arrays

The TS7720 disk subsystem uses disk drives that form part of a Redundant Arrays of Independent Disks (RAID). The number of RAID arrays varies depending on the specific storage capacity of the TS7720. Disk encryption is supported only on recent TS7720 disk subsystem models. The current TS7720 disk subsystem model 3956-CS9 (and its 3956-XS9 expansion drawers) uses RAID6 arrays which can withstand two disk failures in the same array. Additionally, all systems come with spare drives to mitigate disk failures. When a disk fails, a spare drive automatically takes over for the failed drive. When a spare drive has fully taken over, the RAID array is fully protected again. When the failed drive is physically replaced, the new drive will copy over from the spare drive. The spare drive then goes back to being an unused spare drive. This behavior is consistent between encryption capable and non-encryption capable disk subsystems.
When disk encryption is enabled, all disk members of the RAID arrays are individually encrypted. When a spare drive takes over for a failed drive, it automatically turns on its encryption and any data that is being rebuilt will therefore be encrypted on that spare drive. When the failed drive is physically replaced, the replacement drive will also automatically turn on its encryption and permanently form part of the RAID array. The spare drive then goes back to being a spare but will remain encrypted.

With disk encryption enabled the failed drive can be safely disposed of knowing that its contents are encrypted and thus unreadable.
Drives with encrypted data in a RAID array

Unused spare drive with no data

Tape volume

Drives with encrypted data in a RAID array with one failed drive. The failed drive contains encrypted data which will be ineligible if attempted to be read back.

Spare drive in use. Data is encrypted
Key Exchanges and Encryption

When disk encryption is first enabled, all drives, whether used, unused, spare or array members, will be given a key. This key is stored inside the cryptography chipset of the drive. The additional matching key is stored inside the controller’s non-volatile RAM (NVRAM). Any drive will then ask for a key during the first initial I/O such as during power-ups, when a spare drive becomes an array member, etc. If this key does not match the internal key of the drive, the drive will lock up and no further I/O will be allowed.
The encryption itself however is done individually by each drive’s on-board cryptography chipset. The key stored by the drive is not part of the algorithm used to encrypt its contents. The key is instead used to unlock the drive and allow read or write I/O operations. Once the drive is unlocked all write I/O operations will be encrypted by the drive’s cryptography hardware before they get written to physical media. Similarly only drives that are unlocked will be allowed to read from the physical media. The read I/O operations will get decrypted by the drive’s cryptography chipset before being presented to the disk subsystem controllers.

Using this approach enables the TS7720 to protect the data inside the local disk subsystem disks while automating the encryption and the management of the keys in a way that is transparent to the user. Performance is maximized and downtime is minimized by using a hardware based cryptography chipset localized to each individual disk drive.
References

IBM System Storage Installation and Host Support Guide, GA32-0963-01

TS7700 Virtualization Engine Information Center.
http://publib.boulder.ibm.com/infocenter/ts7700ic/v1r0/index.jsp

IBM TotalStorage Virtual Tape Server – Using 3592 In a VTS – Version 5,

IBM Virtualization Engine TS7700 Series Bulk Volume Information Retrieval Function User's Guide Version 1.0,
http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100828

IBM Virtualization Engine TS7700 Series Statistical Data Format White Paper,
http://03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100829
**Disclaimers:**

Copyright © 2012 by International Business Machines Corporation.

No part of this document may be reproduced or transmitted in any form without written permission from IBM Corporation.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This information could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) at any time without notice.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM’s intellectually property rights, may be used instead. It is the user’s responsibility to evaluate and verify the operation of any non-IBM product, program or service.

The information provided in this document is distributed "AS IS" without any warranty, either express or implied. IBM EXPRESSLY DISCLAIMS any warranties of merchantability, fitness for a particular purpose OR NON INFRINGEMENT, IBM shall have no responsibility to update this information. IBM products are warranted according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. IBM is not responsible for the performance or interpretability of any non-IBM products discussed herein. The customer is responsible for the implementation of these techniques in its environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. Unless otherwise noted, IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

The provision of the information contained herein is not intended to, and does not grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Trademarks

The following are trademarks or registered trademarks of International Business Machines in the United States, other countries, or both.

IBM, TotalStorage, DFSMS/MVS, S/390, z/OS, and zSeries.

Other company, product, or service names may be the trademarks or service marks of others.