THE CLIPPER GROUP
Navigator™
Navigating Information Technology Horizons℠
Published Since 1993 Report #TCG2006077 August 28, 2006

IBM Gives Enterprises Options for Encryption

Analyst: Dianne McAdam

Management Summary

When I worked in the datacenter, every month brought new problems to be solved. There were many problems to be solved – performance problems with online databases, difficult migrations to newer versions of operating systems, equipment that always seemed to fail on Friday nights and my personal favorite – a roof that leaked onto a very large and immovable mainframe that we protected with drop cloths and umbrellas until additional help arrived. The mainframe survived but my umbrella did not.

We did not worry much about security in those days. Sure, we password protected our files and put combination locks on the computer room doors. However, we never lost sleep worrying about hackers breaking into systems, or tapes getting lost on the way to Iron Mountain, or laptops being stolen.

But times have changed and data security is on the minds of many IT executives. It should be on every executives mind. Over thirty states have enacted legislation that requires notification of security breaches. It is expected that the federal government will pass similar legislation soon. There is a reason for this legislation – security breaches are news items almost every day. The statistics are staggering. Since last year, Privacy Rights Clearinghouse, a nonprofit consumer advocacy organization, estimates that over 90 million consumers have been notified of potential security breaches regarding their personal sensitive information. Financial institutions must prove that their data is secure. Security breaches violate regulations but can also result in negative publicity and lost business. These breaches are not limited to financial institutions, but can affect hospitals, insurance companies, government agencies – in fact, any company that processes sensitive personal and financial data, including credit/debit card transactions and information. I am not happy to report that I am one of those 90 million consumers.

It is no longer *good enough* to put combination locks on computer room doors or require passwords on files. A large amount of data is still written to tape and shipped off site every day of the year. Business partners need to exchange sensitive data to remain competitive and much of this data is exchanged through tape cartridges. All of this data needs to be secured, and it needs to be secured now.

There have been several different ways to secure tape data through encryption. However, many of the solutions have been point products that have been complex to manage. With IBM's recent announcements, mainframe enterprises now have several options available to ensure that data is now secure. Nevertheless, this announcement in not only for mainframe enterprises; enterprises running various flavors of Unix and Windows can benefit as well. Read on for the details.

IN THIS ISSUE

- IBM's Encryption Announcements 2
- Outboard Tape Drive Encryption 2
- Key Management 2
- Which Method to Choose? 3
- Conclusion 3

IBM's Encryption Announcements

Encrypting data on tape is not new – enterprises have had several options to write encrypted data on tape. (1) Host software can created encrypted data and send it to a tape drive. This takes processing cycles and is limited to encrypting data originating on that host. (2) There are specially built appliances that sit within a SAN. However, many units of these appliances may need to be purchased to support large tape drive environments and the cost of this solution can add up quickly. Now, IBM has announced several offerings that can save enterprises money without affecting performance.

Outboard Tape Drive Encryption

IBM has announced 256-bit AES hardware encryption built into the IBM TS1120 tape drive. Why encrypt at the drive level? The answer is simple – performance and capacity. Hardware encryption always performs better than software encryption. IBM's testing in their labs shows a one percent overhead when encryption is activated.

Encrypted data does not compress well. Compression techniques find and eliminate repetitive characters. Encryption scrambles the data making compression ineffective. The TS1120 drive compresses *then* encrypts the data. If the data was normally compressed at 2- or 3-to-1, it is still compressed at the same ratio. The same amount of data already encrypted then sent to a tape drive may require two or three times more tape cartridges – an added expense.

Encryption support will be standard on all TS1120 tape drives shipped after September 8th and will cost about ten percent more than the older models. Existing TS1120 drives can be upgraded to support encryption.

Key Management

Encrypting data is easy; managing the keys is the hard part. Tape data can be created from several different operating systems such as *z/OS*, Windows, or Unix. Different types of application data, such as email messages or database backups may need to be secured. Secured archival data must be kept for years, or decades and keys have to be accessible until the data is deleted. Data must be secured through encryption keys but keys must also be protected to prevent unauthorized access.

IBM offers three places to manage encryption for the TS1120:

- Operating system (z/OS)
- Tape Library
- Application (Tivoli Storage Manager)

z/OS System Key Management

With this approach, z/OS operating system manages the keys with a new mainframe resident program called *Enterprise Key Manager* or *EKM*. The z/OS operating system has a long history in supporting security and encryption. For example, hardware cryptography was first available over 35 years ago. *RACF*, software to control access to resources, was released in 1976. Key management was built into the operating system with the introduction of *ICSF* in 1991. Last year, the *Encryption Facility for z/OS* was announced, which uses mainframe cryptography to encrypt tape cartridges. Now, the pairing of encryption-capable TS1120 tape drives with EKM provides end-to-end secure tape encryption.

The mainframe also has a long history of reliability and resiliency that makes it a perfect choice for centralizing key management. The following two cases show how centralized key management works with mainframe and open systems servers.

In the first case, a TS1120 tape drive is connected via FICON channels to a z9 or other mainframe with z/OS.

1. z/OS sends a request to encrypt data to the tape drive.
2. The tape drive requests a key from z/OS.
3. EKM uses existing security policies and hardware cryptography to generate a unique key for each cartridge and encrypts that key with public and private keys.
4. The unique key is sent back to the tape drive, which writes the encrypted data and the encrypted key on the cartridge.

IBM uses a hierarchical key structure to provide security. The public and private keys are stored on the host in existing key-stores such as ICSF, while the unique data key is stored in encrypted form on the tape cartridge.

z/OS can also manage the keys for open systems platforms that write data to tape. In this second case, the TS1120 is connected via Fibre Channel to an open systems server. The tape library has an IP connection to the z/OS mainframe.

1. The open systems operating system requests the tape drive write encrypted data.
2. The library management software requests a key from the EKM resident on the z/OS operating system via an IP socket connection.

Copyright © 2006 by The Clipper Group, Inc. Reproduction prohibited without advance written permission. All rights reserved.

3. The EKM generates the unique data keys, encrypts the data key, and send the unique keys back to the tape drive just as described in the first case above.

A second version of z/OS can serve as a secondary key manager and share the same key-store for redundancy, via *Sysplex* data sharing. The Primary and Secondary Key manager can also have different key-stores that are kept in sync through mirroring. This can provide disaster recovery capabilities, ensuring that in a disaster, keys can be decrypted and data can be read at remote locations.

Since May 2004, every central processor that ships with a zSeries 990 or 890 server comes with a built in assist for cryptography. Crypto Express2 is a third-generation cryptographic feature that ensures that key information is never "in the clear" in system memory.

Tape Library Key Management

This approach is designed for enterprises that do not have z/OS systems and do not want to bring in a z/OS system to manage keys. IBM's Java-based Enterprise Key Manager can run on many different server platforms besides z/OS, including *AIX*, *HP-UX*, *Solaris*, *Windows*, *Linux*, and *i5/OS*. In this example, a TS1120 tape drive is connected to a Windows server via Fibre Channel.

1. An application running on Windows requests a mount of a tape cartridge by volume serial number. Specific tape cartridges, by volume serial numbers, are designated as having encryption turned "on".
2. The tape library requests a key from the EKM residing on another server.
3. EKM supplies the unique data key and public-key encrypted data key to the library.
4. The application starts writing data to the tape drive to be encrypted, and the data key is also stored on the tape in encrypted form.

Application Key Management

This third approach may appeal to IT administrators that are already using application-based encryption. For example, *Tivoli Storage Manager (TSM)* has supported software-based encryption for years. However, software-based encryption consumes processor cycles. TSM now is integrated with the new TS1120 and can now use the more efficient hardware-based encryption on the TS1120, while continuing to manage the keys within TSM.

Which Method to Choose?

Which method is the right method to choose? The answer depends on the environment and the need to interchange data with other companies.

Mainframe only environments will find that managing keys on the mainframe can simplify management, since the new Encryption Manager works with existing DFSMS and RACF policies. When paired with the TS1120, performance will remain the same without requiring additional tape cartridges. Environments with z/OS and other server platforms connected to TS1120 drives will find that z/OS key management provides a single point of control for all platforms.

Enterprises without mainframes can use library-based key management. Enterprise Key Manager running on its server will manage all keys.

Data centers already using TSM for encryption will find that pairing TSM with the TS1120 will speed up the encryption process and provide additional capacity relief since data can now be first compressed, then encrypted.

Enterprises that exchange data and have encryption-capable TS1120 tape drives installed in both locations can exchange encrypted TS1120 tape cartridges. Enterprises that exchange data and do not both have encrypting TS1120 tape drives can exchange encrypted data by using IBM's Encryption Facility for z/OS to encrypt on the host and manage the distribution of keys.

Conclusion

Ensuring that customer sensitive data is protected is the responsibility for every IT organization. Many enterprises have implemented point solutions that are difficult to manage and maintain. IBM's new encryption announcements now give data centers a choice. Keys can be managed within the z/OS operating system, through library management services or within integrated applications, such as TSM.

You now have more and better choices from which to choose your preferred method(s) to encrypt what needs to be secured. Excuses for not moving forward will no longer be accepted!

Copyright © 2006 by The Clipper Group, Inc. Reproduction prohibited without advance written permission. All rights reserved.

About The Clipper Group, Inc.

The Clipper Group, Inc., is an independent consulting firm specializing in acquisition decisions and strategic advice regarding complex, enterprise-class information technologies. Our team of industry professionals averages more than 25 years of real-world experience. A team of staff consultants augments our capabilities, with significant experience across a broad spectrum of applications and environments.

- ***The Clipper Group can be reached at 781-235-0085 and found on the web at www.clipper.com.***

About the Author

Dianne McAdam **is Director of Enterprise Information Assurance for the Clipper Group**. She brings over three decades of experience as a data center director, educator, technical programmer, systems engineer, and manager for industry-leading vendors. Dianne has held the position of senior analyst at Data Mobility Group and at Illuminata. Before that, she was a technical presentation specialist at EMC's Executive Briefing Center. At Hitachi Data Systems, she served as performance and capacity planning systems engineer and as a systems engineering manager. She also worked at StorageTek as a virtual tape and disk specialist; at Sun Microsystems, as an enterprise storage specialist; and at several large corporations as technical services directors. Dianne earned a Bachelor's and Master's degree in mathematics from Hofstra University in New York.

- ***Reach Dianne McAdam via e-mail at dianne.mcadam@clipper.com or at 781-235-0085 Ext. 212. (Please dial "212" when you hear the automated attendant.)***

Regarding Trademarks and Service Marks

The Clipper Group Navigator, **The Clipper Group Explorer**, **The Clipper Group Observer**, **The Clipper Group *Captain's Log***, **The Clipper Group Voyager**, and *"clipper.com"* are trademarks of The Clipper Group, Inc., and the clipper ship drawings, "*Navigating Information Technology Horizons*", and "*teraproductivity*" are service marks of The Clipper Group, Inc. The Clipper Group, Inc., reserves all rights regarding its trademarks and service marks. All other trademarks, etc., belong to their respective owners.

Disclosure

Officers and/or employees of The Clipper Group may own as individuals, directly or indirectly, shares in one or more companies discussed in this bulletin. Company policy prohibits any officer or employee from holding more than one percent of the outstanding shares of any company covered by The Clipper Group. The Clipper Group, Inc., has no such equity holdings.

Regarding the Information in this Issue

The Clipper Group believes the information included in this report to be accurate. Data has been received from a variety of sources, which we believe to be reliable, including manufacturers, distributors, or users of the products discussed herein. The Clipper Group, Inc., cannot be held responsible for any consequential damages resulting from the application of information or opinions contained in this report.

Copyright © 2006 by The Clipper Group, Inc. Reproduction prohibited without advance written permission. All rights reserved.