BRMS Encryption

By Garth Tucker

In the last number of years, many businesses have been legislated or taken upon themselves to secure their data. However, one piece of this that was often overlooked is offsite data. Onsite data is hidden behind firewalls and may have numerous levels of authority securing it, but when it goes offsite on tapes or through other electronic means, it has been essentially available to anyone who nicked a tape. This has been a bit of a black-eye for some enterprises, which shall remain nameless, when tapes or in one case, disk units went missing, with not just critical business data, but individuals personal data as well. This contravenes privacy laws that have been enacted over the last several years, such as SOX, Visa PCI, HIPAA and PIPEDA here in Canada.

In response to this issue, IBM began identifying ways and means to alleviate the issue with offsite data on tape storage or "Data at Rest". Data being sent over a network or other such method is identified as "Data in Motion" and is secured through other means such as SSL, which we will not get into in the scope of this discussion.

Through use of encryption (also known as cryptography), we can secure the data being stored on tapes. On the i5, we can utilize the encryption standard AES 256, which Wikipedia defines as Advanced Encryption Standard (AES), also known as Rijndael, a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process. It became effective as a standard May 26, 2002. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. It is available by choice in many different encryption packages. The cipher was developed by two Belgian cryptographers, **Joan Daemen** and **Vincent Rijmen**, and submitted to the AES selection process under the name "Rijndael", a portmanteau of the names of the inventors.

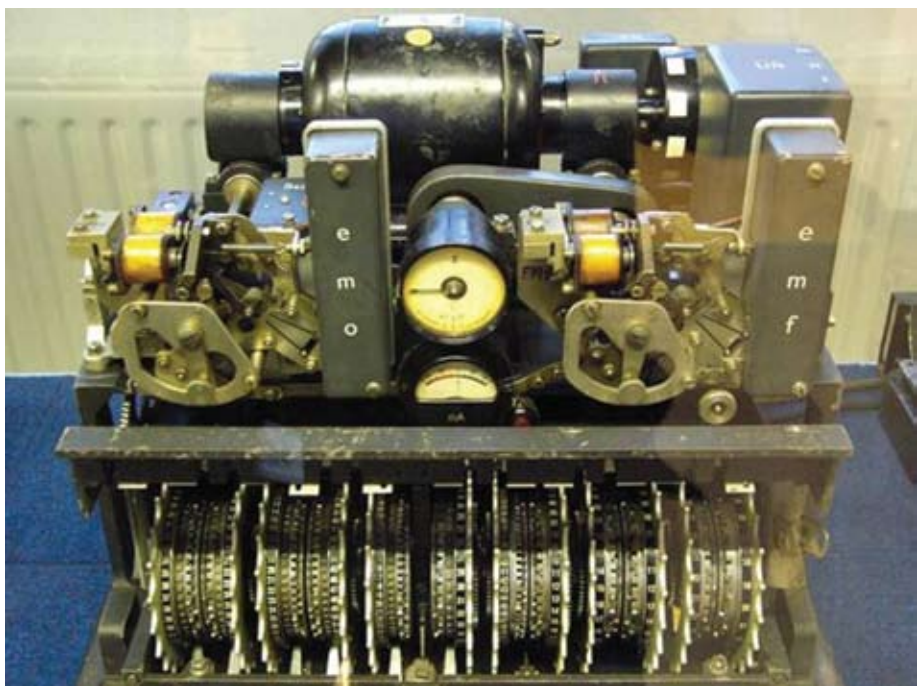
So what does all this mean to us? If we want to secure our tapes going offsite, we have a couple of methods from IBM:

1. Hardware capable tape devices with an EKM (Encryption Key Manager), or with V6R1:
2. Software Encryption using BRMS Advanced (5761BR1 – Option 2) and Cryptographic Services Key Management.

Both of these methods have pros and cons and you will need to assess your requirements to determine which method works best for you. For our purposes here, we will focus on Software Encryption using the BRMS Advanced function.

This encryption solution is hardware independent, meaning no need for any encryption device. To use the function, you need to have the BRMS Advanced feature (5761-BR1 Option 2) and Cryptographic Service Provider (5761-SS1 Option 35) installed on the operating system. Previously, the Advanced function (Option 2) of BRMS allowed you to perform Hierarchical Storage Management (HSM) functions and now contains the functions to allow us to perform encryption.

This is a chargeable feature and you should check with your IBM or IBM Business Partner rep for pricing. Cryptographic Service Provider – Option 35 is an optional part of the OS and again, you will have to check with your IBM or IBM Business Partner rep for pricing.



Enabled encryption will be supported for any tape library, standalone tape drive, virtual tape and media duplication. This means that we can avoid changing tape platforms if it's not convenient at this time.

All user data may be encrypted, but Operating System objects and tape labels will not be encrypted. This may be the biggest drawback to this method over using a hardware solution. This may or may not meet with your auditing/security requirements and you should investigate this with your auditors prior to committing to implementation. In my opinion, if you configure your backups to only send user data offsite, you will be meeting the spirit of the legislation.

Performance Considerations

Software encryption will require additional processor capacity. From my experience with the product during the V6R1 Technical Overview, it adds significant overhead to your saves. However, my thinking is that this can be dealt with through the use of the Save-While-Active function and being creative with your backup control groups.

Encrypting

According to the InfoCenter, cryptographic services key management for the i5/OS operating system allows you to store and manage master keys and keystores. On the i5, Cryptographic Services supports a hierarchical key system. At the top of the hierarchy is a set of master keys. These keys are the only key values stored in the clear (unencrypted). Cryptographic services securely stores the master keys within the i5/OS Licensed Internal Code. Eight general-purpose master keys are used to encrypt other keys which can be stored in keystore files. Keystore files are database files. Any type of key supported by cryptographic services can be stored in a keystore file, for example AES, RC2, RSA, SHA1-HMAC.

In addition to the eight general-purpose master keys, cryptographic services supports two special-purpose master keys. The ASP master key is used for protecting data in the Independent Auxiliary Storage Pool (in the Disk Management GUI is known as an Independent Disk Pool). The save/restore master key is used to encrypt the other master keys when they are saved to media using a Save System (SAVSYS) operation. BRMS will not manage the keys used for encryption, meaning you must provision to allow for key management. It provides the interface for the user to ask for encryption, specify the keys to use for the encryption and what items to be encrypted. The key information is also saved by BRMS and BRMS knows what key information is needed to decrypt on the restore.

Conclusion

We know now that we can use BRMS and software encryption to secure user data that is going offsite and generally how it works, but it must be determined by your requirements and the businesses auditing requirements as to whether or not this will meet your needs. As far as I can see, this will suffice for most SMB clients and give them the level of security for their "Data at Rest" without having to migrate to a newer tape technology or invest in an EKM server. It's easy to implement and provides a level of security that is currently not in place for clients who do not have budget for hardware changes. TUG

***Garth Tucker**, the managing director of i3 Tech Group and Dynamic Disaster Recovery of Aurora, is an IBM System i Specialist and Business Continuity Planner. IBM Certified for V4R3 through V5R4 as well as being CompTIA Linux+ Certified. He has many years of experience with AS400, iSeries and now i5 and helped write the Technical Overviews of OS400; V4R4, V4R5, V5R1 and V6R1 with the IBM ITSO. In addition, he has written numerous articles for the Toronto Users Group, Midrange Magazine and COMMON.CONNECT magazine and has presented sessions at COMMON, the Toronto Users Group's TEC conference and Meetings of Members.*