Virtual IMS user group: Newsletter 65

Welcome to the Virtual IMS user group newsletter. The Virtual IMS user group at www.fundi.com/virtualims is an independently-operated vendor-neutral site run by and for the IMS user community.

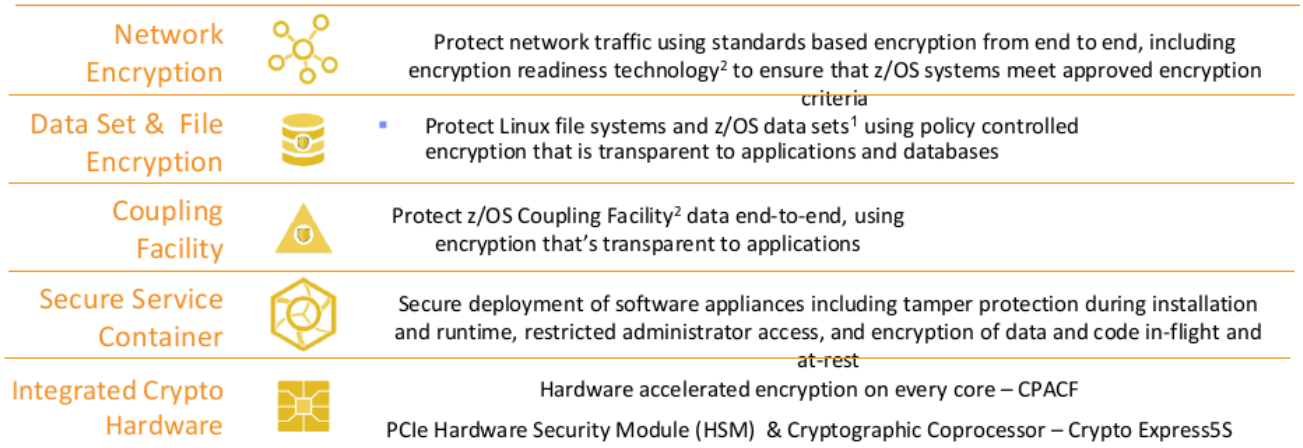


Figure 1: Pervasive Encryption with IBM Z

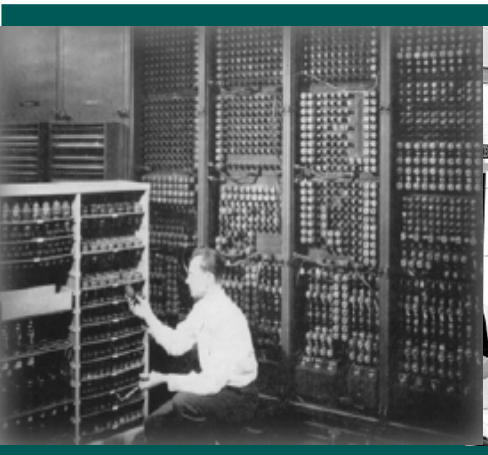
Virtual IMS user group presentation

The latest webinar from the Virtual IMS user group was entitled, "Pervasive Encryption and IMS". It was presented by Dennis Eichelberger, IT Specialist, IMS Support - Washington Systems Center, IBM.

Dennis has over 35 years of 'mainframe' operating and database systems experience. He has worked as a developer, a consultant, business partner, and vendor to IBM. Dennis is currently a member of the IMS Support team of the Washington Systems Center. His spare time is spent practicing the Gentle Way.

Dennis Eichelberger started his presentation by observing that data protection and

Contents:



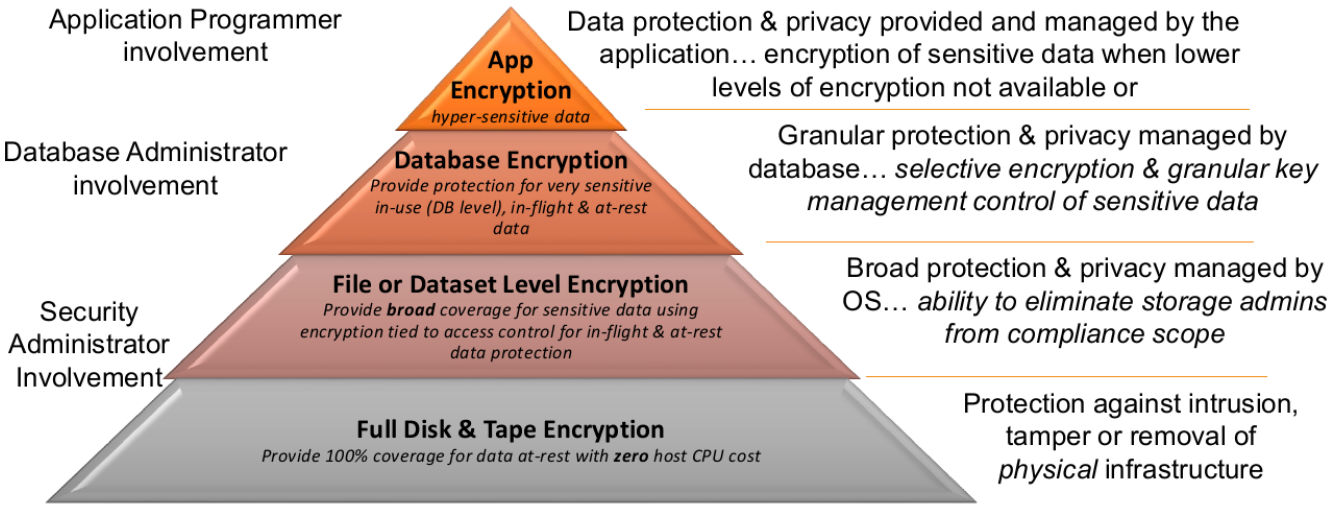


Figure 2: Levels of encryption

compliance are business imperatives. There's a 26 percent likelihood of an organization having a data breach in the next 24 months. And of the 9 billion records breached since 2013, only 4 percent were encrypted. The average cost of a data breach in 2016 was $4M. There are also standards that organizations need to comply with such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI-DSS), and the more-recent European Union General Data Protection Regulation (GDPR). In terms of data breaches, "It's no longer 26% a matter of if, but when ...".

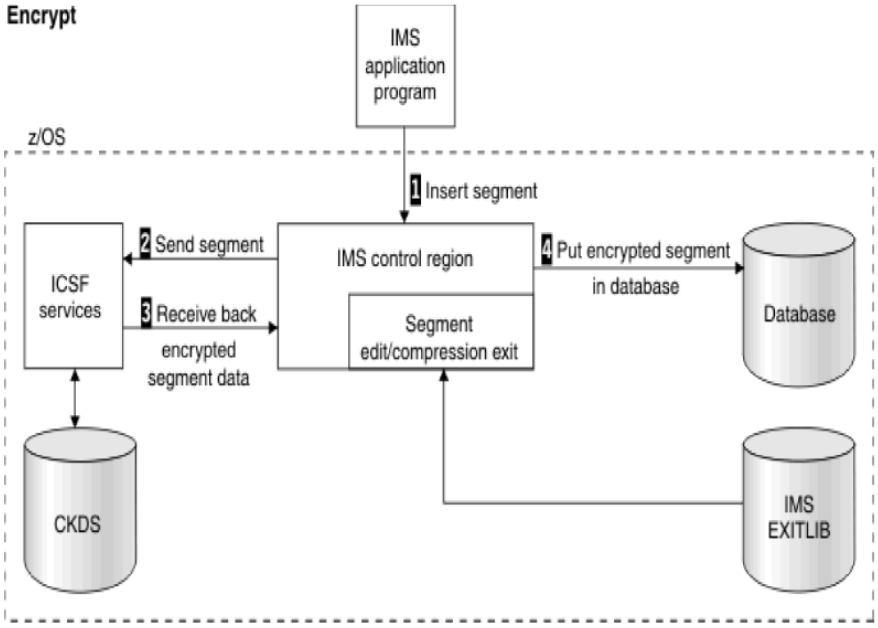
In 2016, the average time before a breach was discovered was 191 days. And that just illustrates the need for encryption. Figure 1 illustrates how pervasive encryption with IBM Z is enabled through tight platform integration.

Figure 2 shows that the levels of encryption depend on where the data needs to be encrypted, and implementation depends on resources and expected results.

The Integrated Cryptographic Service Facility (ICSF) provides z/OS integrated software support for data encryption, and an operating system software API Interface to Cryptographic Hardware. And the hardware gets faster on each processor model. There's enhanced key management for key creation and distribution – this includes public and private keys, secure and clear keys, and master keys. The created keys are stored/accessed in the Cryptographic Key Data Set (CKDS) with a unique key label. The CKDS itself is secured using the Security Access Facility.

Master keys are used to generate, encrypt, and store user keys into the CKDS. They are loaded into the CEX*nn* hardware, and stored nowhere else. User keys (data encrypting keys) are generated via ICSF services, stored inside the CKDS, may be public or private, clear or secure, and are used by the IBM InfoSphere GDEz Encryption Tool along with the encryption algorithm to convert user data to ciphertext for database encryption.

A clear key is exposed in the storage of a processor and can be viewed in a dump of storage. If this is correctly interpreted, it can expose data. It's used in software-



1. IMS application program passes a segment REPL, ISRT, or LOAD request to the IMS control region. IMS uses the DBD to determine that a Segment Edit/Compression exit is required, so IMS loads the exit.
2. Exit invokes ICSF services, passing user-defined data encryption key label (provided by exit) and unencrypted segment.
3. When the segment has been successfully encrypted, the exit passes the segment back to IMS.
4. IMS then puts the encrypted segment into the database

Figure 3: IMS encryption flow

based cryptography, so used by CPACF and the CEX*n* hardware is not required. A secure key is only ever exposed in bounds of a secure processor and can never be seen in storage or a dump. It is held encrypted under the master key. APIs are available via ICSF, and it can be used from Java on z/OS.

Application encryption requires changes to applications to implement and maintain. It is highly granular and protects data right up to the point where it will be used. The applications must be responsible for key management, and it's a suitable technique for selective encryption of hyper-sensitive data.

Database encryption encrypts sensitive data at the Db2 row and column levels and IMS segment level. It is transparent to applications. It requires Separation of Duties (SOD) and granular access control. It protects Data-In-Use within memory buffers, and clear text data cannot be accessed outside DBMS access methods. The sensitive data in logs, image copy data sets, and DASD volume backups are also encrypted. It utilizes IBM Z integrated cryptographic hardware. Figure 3 illustrate IMS encryption flow.

When working with IMS, some things to think about are:

- ICSF initialize with CHECKAUTH = NO

  If these options are set to YES it will invoke an extended path length
- A separate segment Edit/Compression exit needs to be built for each separate cryptographic key label
- A single key label may be used for multiple segments
- APF authorize the dataset containing the segment edit routines
- IMS loads the segment Edit/Compression routines below the 16M line
- Be aware of storage use
- IMS databases allocated using OSAM dataset currently are encrypted ONLY by Guardium.

Data set encryption is: enabled by policy; transparent to applications; tied to access control; and uses protected encryption

Data Set Type	Notes	Address Space Userids Needing Key Label Access*
Database: VSAM (HALDB, non-HALDB)	Extended addressability attribute not supported for VSAM DBs.	CTL, DLI, batch jobs, utilities accessing DB
Database: DEDB	Added with APAR PI83756 PTF UI53418	CTL, DLI, batch jobs, utilities accessing DB
WADS (DFSWADSn)	VSAM Linear dataset. Must be allocated in Extended Format	CTL (including XRF alternate, FDBR regions), log archive utility, other utilities accessing OLDS, RSR transport manager
Online log data sets (DFSOLPnn, DFSOLSnn)		CTL (including XRF alternate, FDBR regions), log archive utility, other utilities accessing OLDS, RSR transport manager
Batch log data sets		CTL (including XRF alternate, FDBR regions), log archive utility, other utilities accessing OLDS, RSR transport manager
SLDS / RLDS		IMS batch jobs, utilities accessing batch logs, RSR transport manager

Data Set Type	Notes	Address Space Userids Needing Key Label Access*
Change Accum data sets	Change accumulation utility, DB recovery utilities	Change Accumulation data sets
Image copy data sets	Image copy utilities, DB recovery utilities	Image copy data sets
CQS SRDS		CQS
IMS Connect Recorder Trace		IMS Connect, utilities that process IMS recorder trace
BPE Trace data sets	Need to use RACF rules or DATACLAS with key label. Key label is not supported by BPE EXTTRACE statement.	Address spaces that use BPE, utilities that process BPE trace data (including IPCS TSO users)
z/OS log stream offload and staging data sets	Dependent on z/OS logger encryption support	z/OS logger address

Figure 4: IMS V15 data sets supported in the DFSMS data set encryption

Data Set Type	Notes
Database: OSAM	EXCP / custom channel program; cannot be extended format
MSDB data sets	IBM has recommended MSDBs be converted to DEDBs for the last 10 IMS releases.
Queue manager data sets (LGMSG, SHMSG, QBLKS)	Uses OSAM
Restart data set (RDS)	Uses OSAM
All PDS / PDSE type data sets (PSBLIB, DBDLIB, ACBLIB, MODBLKS, FMTLIB, IMSTFMTx, IMSDALIB, program libraries, PROCLIB/configuration data sets, catalog directory, staging, BSDS)	DFSMS does not support PDS/PDSE encryption
Spool data sets	EXCP / custom channel program; cannot be extended format

Figure 5: Encryption is explicitly *not* supported for the following IMS V15 data sets

keys. It can be used to broadly encrypt data at rest. It covers VSAM, Db2, IMS, middleware, logs, batch, and ISV solutions. It can encrypt in bulk, for low-overhead, and utilizes the integrated cryptographic hardware. With data set encryption, no application changes are required. A data set is defined as 'encrypted' when a key label is supplied either on or prior to allocation of a new sequential or VSAM extended format data set.

Hardware encryption provides protection against intrusion, tamper, or removal of physical infrastructure. It protects at the DASD subsystem level. It provides all or nothing encryption, but only data at rest is encrypted. A single encryption key is used for everything. There's no application overhead and zero host CPU cost. It prevents exposures on: disk removal, box removal, and file removal.

DFSMS data set encryption is established for a given data set when that data set is created and has a key label associated with it. Encrypted data sets must be extended format. Key labels can be specified for a data set by:

1 Creating RACF rules that associate a key label with a data set name pattern, via the DATAKEY parameter of the DFP segment.

2 Specifying a key label directly on JCL, dynamic allocation, TSO allocate, or IDCAMS DEFINE

3 Using a DATACLAS with a key label associated with it

Existing (already created) data sets that are not encrypted do not become encrypted just because their DATACLAS has a key label added to it, or because a RACF rule associates a key label with the data set. Existing data sets must be copied into a new extended format data set defined with a key label to become encrypted.

Dennis had a number of encryption implementation considerations. They were:

- Application
  - Application logic determines which key to use for each field/ column

  - Password is managed by the application
- Data Administrator - Data Encryption Tool
  - Sets up the EDITPROC and specifies the key to be used for the entire table – Db2
  - Sets up the COMPRTN and specifies the key for encrypted segments – IMS
  - Key must be defined to/managed by ICSF (stored in the CKDS)
- Security requirements
- Performance requirements
  - Single transaction vs bulk processes
- Application/production support
- Space considerations
- Crypto hardware available
- Not insignificant
  - Multiple points of implementation
- May require multiple groups to coordinate
  - Security
  - Storage
  - System programmer
- Have a back up / back out plan.

A copy of Dennis Eichelberger's presentation is available for download from the Virtual IMS user group Web site at www.fundi.com/virtualims/presentations/IMSPervasiveEncryptionDec18.pdf.

You can see and hear the whole user group meeting at https://youtu.be/rh0mvrsn8XI.

Meeting dates

- On 5 February, Kevin Hite, Senior Technical Staff Member (STSM) - IMS Architect at IBM will be looking at "IMS ODB".
- The following meeting will be on 9 April 2019 when Scott Quillicy will be speaking about data migration.

Recent IMS articles

Is your IMS restart taking too long? Could it be hung? by Sandy Stoob on z Systems Developer Community (30 November2018). You can find the article at https://developer.ibm.com/zsystems/2018/11/30/is-your-ims-restart-taking-too-long-could-it-be-hung-2/

Arcati Mainframe Yearbook

The brand new Arcati Mainframe Yearbook will be available shortly. It includes an annual user survey, an up-to-date directory of vendors and consultants, a resources guide, a strategy section with papers on mainframe trends and directions, a glossary of terminology, and a mainframe evolution section.

Go to https://www.arcati.com/newyearbook19 to visit the download page. The Yearbook is available in PDF format and is completely FREE.

About the Virtual IMS user group

The Virtual IMS user group was established as a way for individuals using IBM's IMS hierarchical database and transaction processing systems to exchange information, learn new techniques, and advance their skills with the product

The Web site at www.fundi.com/virtualims provides a central point for coordinating periodic meetings (which contain technically-oriented topics presented in a webinar format), and provides articles, discussions, links, and other resources of interest to IBM IMS practitioners. Anyone with an interest in IMS is welcome to join the Virtual IMS user group and share in the knowledge exchange.

To share ideas, and for further information, contact trevor@itech-ed.com.

The Virtual IMS user group is free to its members.