Db2 for z/OS
Early experiences using
Transparent Data Set Encryption

Support for z/OS Data Set Encryption

Jim Pickel (pickel@us.ibm.com)
Db2 for z/OS Development

Disclaimer

IBM’s statements regarding its plans, directions and intent are subject to change or withdrawal without notice at IBM’s sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products many not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our product remains at our sole discretion.

Agenda

- Delivering pervasive encryption
- Setting up your encryption key labels
- Steps to protect Db2 system objects
- Steps to protect a Db2 table
- Current Delivery Schedule

Data protection and compliance are business imperatives

"It's no longer a matter of if, but when …"

26%

Likelihood of an organization having a data breach in the next 24 months [1]

European Union General Data Protection Regulation (GDPR)

Of the **9 Billion** records breached since 2013

only **4%** were encrypted [3]

Payment Card Industry Data Security Standard (PCI-DSS)

$4M

Average cost of a data breach in 2016 [2]

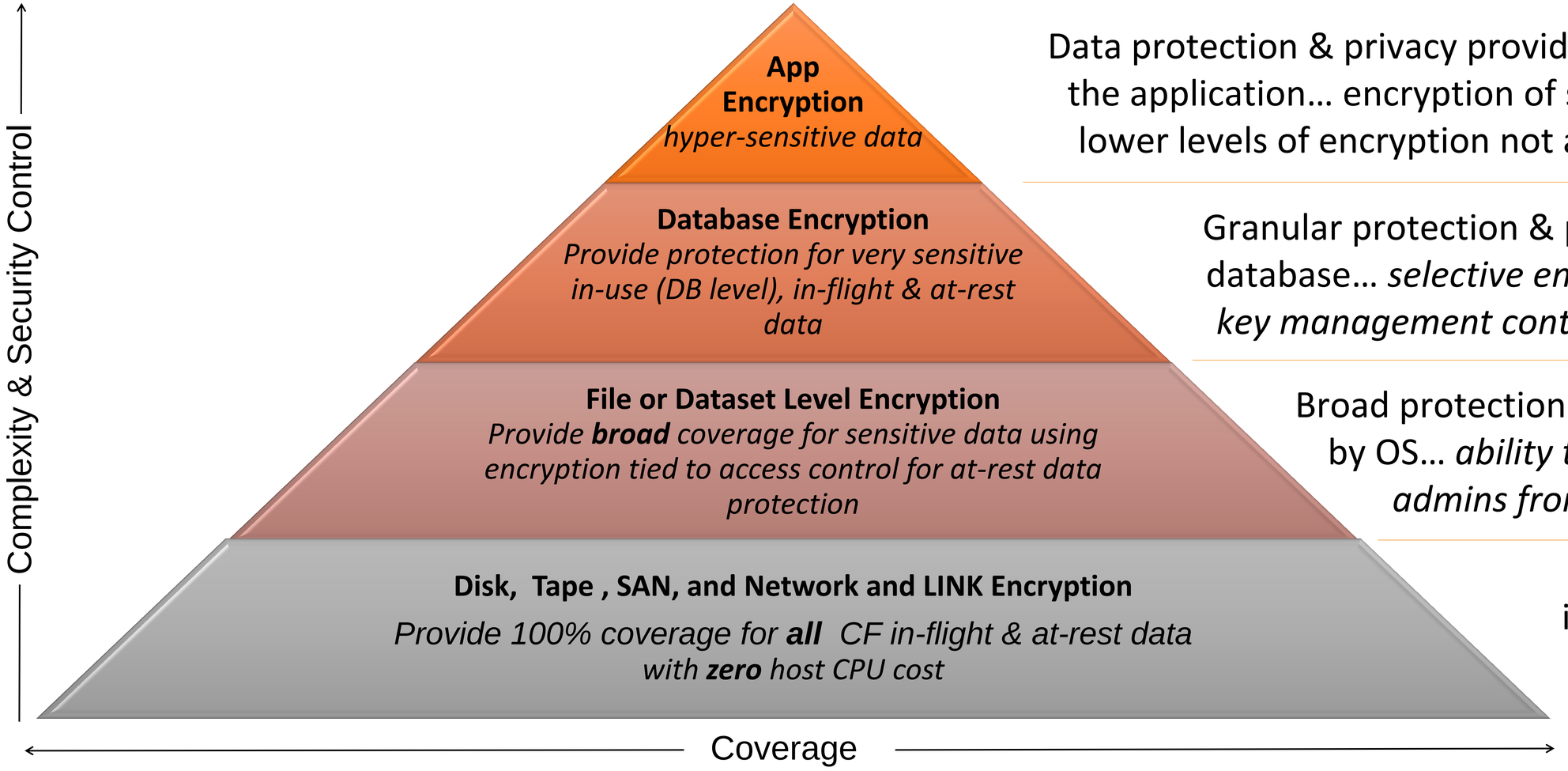
Only **2%** of corporate data Is encrypted vs. 82% of mobile device data [3]

Health Insurance Portability and Accountability Act (HIPAA)

1, 2 Source: 2016 Ponemon Cost of Data Breach Study: Global Analysis -- http://www.ibm.com/security/data-breach/
3 Source: Breach Level Index -- http://breachlevelindex.com/

Multiple Layers of Encryption

Robust data protection



Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

Protection against intrusion, tamper or removal of *physical* infrastructure

Db2 Support of z/OS Pervasive Encryption

- Db2 can now transparently encrypt data at rest without database downtime or requiring the administrator to redefine objects which could cause disruption to operations.

- Utilizes new z/OS DFSMS data set encryption support delivered in z/OS 2.3 and retrofitted back to z/OS 2.2

DFSMS data set encryption

- **DFSMS encrypts/decrypts records when written to or read from disk**
- **Encryption type – AES 256 bit key (XTS, protected key)**
- **Key label** – A 64-byte label of a key in the ICSF CKDS that is to be used for the encryption/decryption
- **Data sets are created as encrypted by specifying key label:**
  - SAF data set profile
  - JCL, Dynamic Allocation, TSO Allocate, IDCAMS DEFINE
  - SMS DATACLAS
- **Application transparency**
  - Data remains encrypted during backup/recovery, migration/recall, and replication
  - In memory system or application data buffers remain in the clear
  - Access to the key label is controlled through SAF permissions, in addition to traditional data set permissions

Db2 Scenarios to enable encryption

Steps to protect a Db2 for z/OS subsystem or group

1. Encrypt your active and archive log datasets
2. Encrypt your catalog and directory tablespaces
3. Encrypt storage groups or specific tables

Setting up your encryption key labels

- ICSF Admin defines encryption key and key label
- Security Admin authorizes Db2 use of the key label
- Options to define a key label used by Db2 (Precedence Order):

1. Security Administrator can set key labels in the data set profiles
2. Database Administrator can set Db2 key labels (V12R1M502 only)
3. Storage Administrator can set key labels in the DFSMS data classes

Encrypting Your Db2 System Objects

Active and Archive log

- While member is stopped, copy the contents of the active log data set to an encrypted data set, restart member
- New archive logs automatically encrypted based on key label settings
- -DISPLAY LOG command to obtain current key label information for each active log data set (V12R1M503)
- -DISPLAY ARCHIVE to obtain current key label information for each archive log data set (V12R1M503)

Catalog and Directory

- Run REORG TABLESPACE utility against catalog and directory table spaces
- Run REPORT TABLESPACESET utility to display key label associated for each catalog and directory table spaces (V12R1M503)

Encrypting Tables

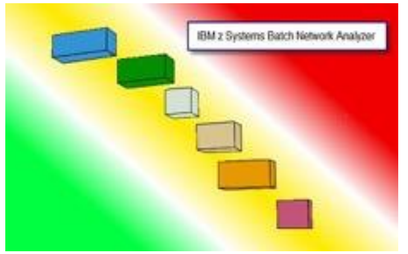
- Set the DATALABEL in data set profile or KEYLABEL in data class
- Run the REORG utility against the tablespaces and indexes
  - Utility job must specify a user ID must have access to any input or output encrypted data sets
  - Utility job uses Db2 authority to access Db2 data sets

Db2 Controls using V12 Function Level M502

- Issue a CREATE or ALTER TABLE to add a key label for individual tables
- Issue a CREATE or ALTER STOGROUP to add a key label for tables in a storage group
- Execute the REORG utility against the tablespaces.
  - Utility job must specify a user ID must have access to any input or output data sets
  - Utility job uses Db2 authority to access Db2 data sets
- Run REPORT TABLESPACESET utility to display key label info for the table spaces used by each table

Estimating CPU Cost of Data Protection

zBNA 1.8.1



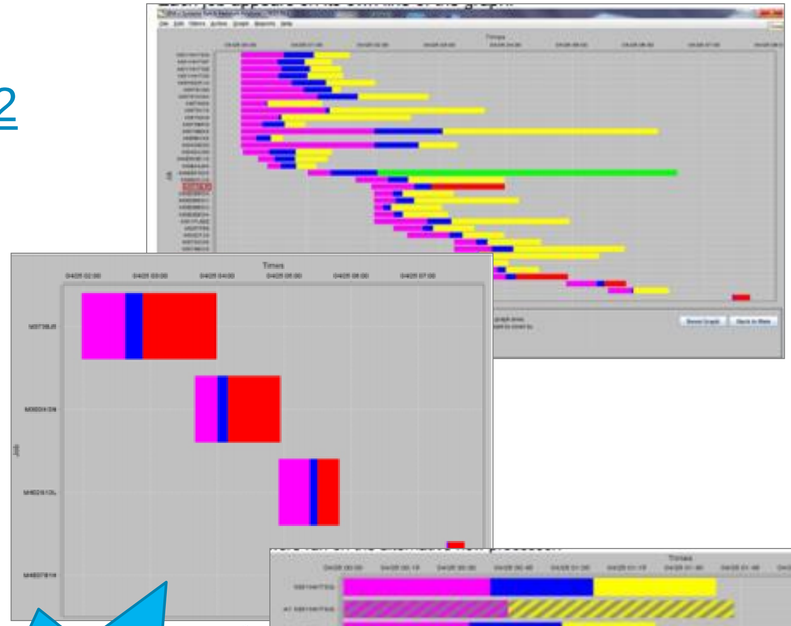
z Batch Network Analyzer (zBNA)

zBNA Background:

- A no charge, “as is” tool originally designed to analyze batch windows
- PC based, and provides graphical and text reports
- Available on techdocs for customers, business partners, and IBMers http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132
- Previously enhanced for zEDC to identify & evaluate compression candidates

zBNA Encryption Enhancements:

- zBNA will be further enhanced to help clients estimate encryption CPU overhead based on actual client workload SMF data
- Ability to select z13 or z14 as target machine
- Support will be provided for
  - z/OS data set encryption
  - Coupling Facility encryption



Version 1.8.1 Available on 8/31/2017

Delivery Schedule

z/OS DFSMS Encryption support

- z/OS 2.1 Support *for coexistence only*
- z/OS 2.2 Data Set Encryption Retrofit
- z/OS 2.3 Pervasive Encryption Support

- **Db2 11 & 12 Base Support**
  - Db2 11 APAR PI81900
  - Db2 12 APAR PI81907

- **Db2 11 & 12 M502 New Function Level (Continuous Delivery)**
  - V12R1M502 – planned availability around Nov, 2017

Important Things to Consider:

- Your key management system must be fully deployed across the enterprise. This step has shown to be the most complicated aspect of deploying pervasive encryption.
- Make sure all IDs used for disaster have access to any key labels used to protect Db2 data sets on all sites.
- For Db2 11 and Db2 12, a key label can be defined by the security administrator or storage administrator, a data base administrator can use Db2 REORG utility to seamlessly migrate Db2 data sets to encrypted data sets with no application outages
- For Db2 12, a new function level will be available to provide new Db2 interfaces to configure and manage Db2 key labels.

Questions?

Thank you!