z/TPFDF Encryption

Communications Subcommittee

Chris Filachek
z/TPF and z/TPFDF Architecture & Development

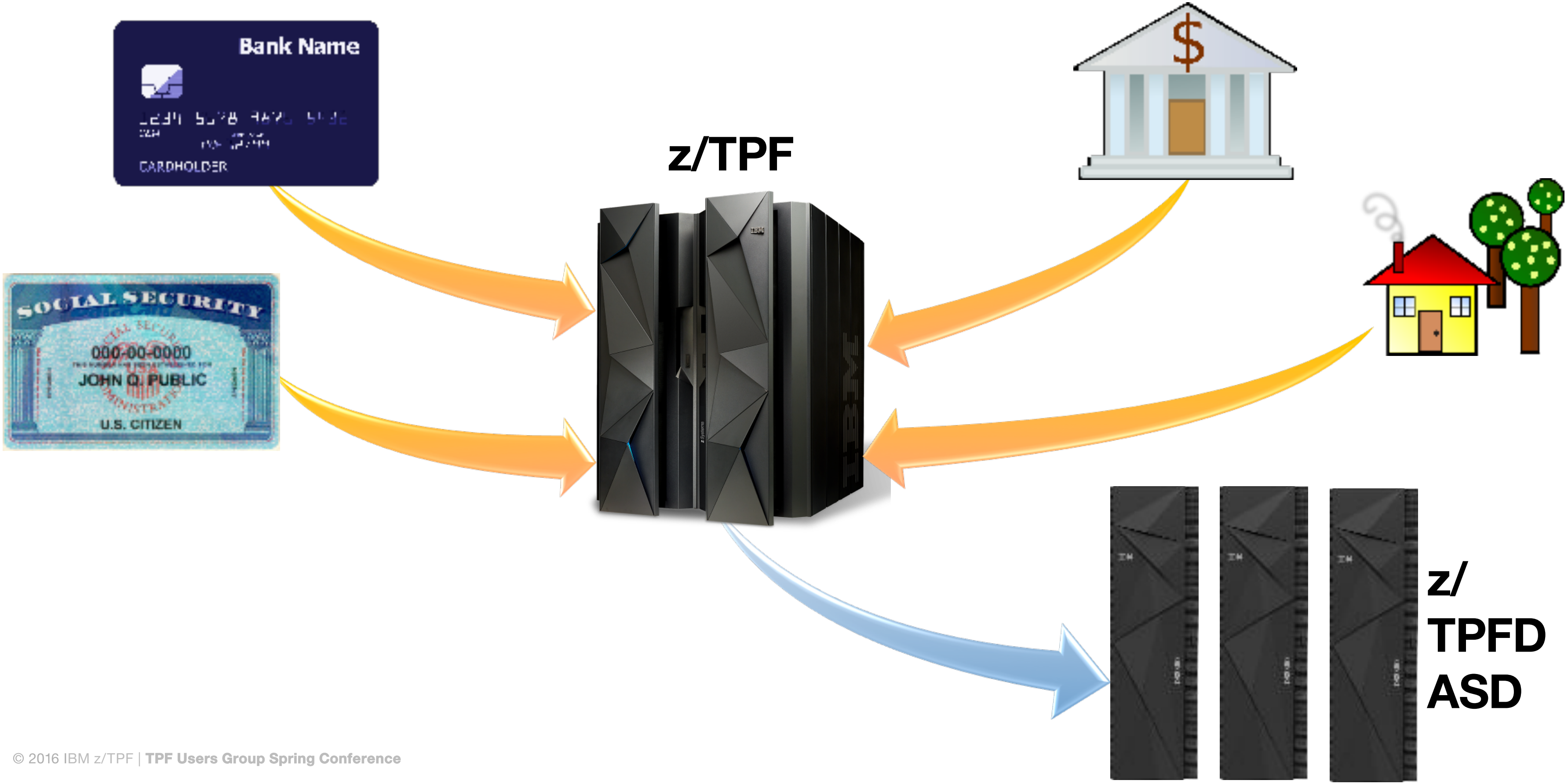
IBM **z/TPF**

April 11, 2016

Disclaimer

Any reference to future plans are for planning purposes only. IBM reserves the right to change those plans at its discretion. Any reliance on such a disclosure is solely at your own risk. IBM makes no commitment to provide additional information in the future.

Sensitive Information in your Systems



z/TPF

z/TPFD ASD

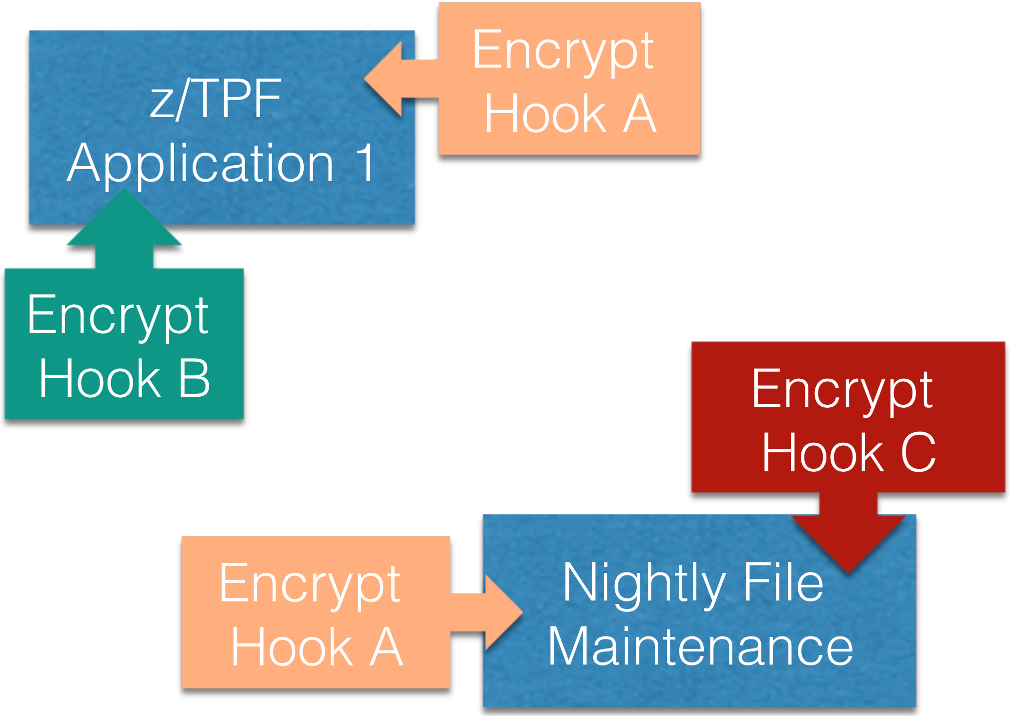
Why secure your data?

- Regulatory requirements
- Corporate security requirements
- Limit financial and non-financial risks from security breaches

As-Is: Securing Sensitive Information

Option 1: Update Applications

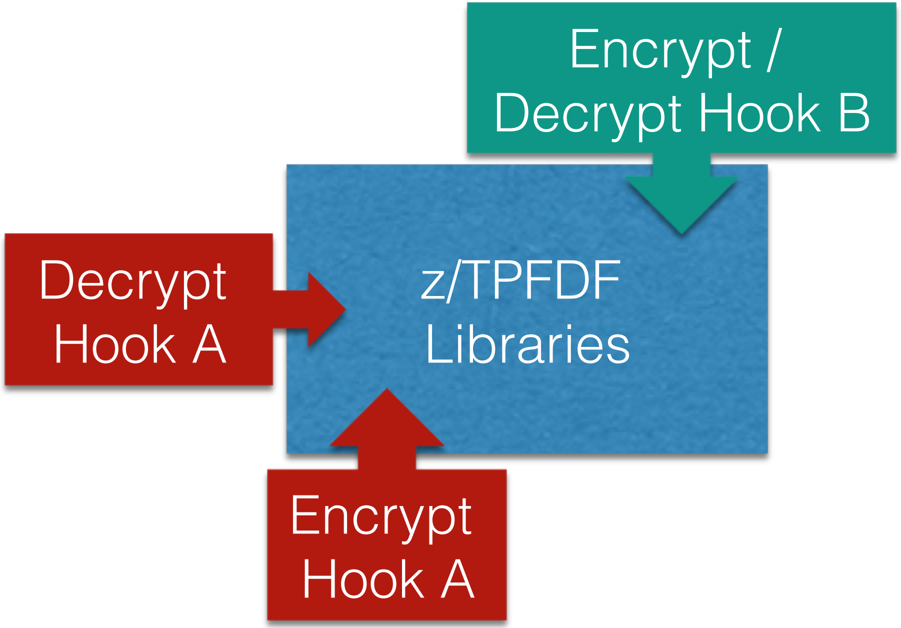
- **Potentially large number of updates - Must update all applications that access encrypted data**
- **May require unique hooks for each database**
- **Ongoing maintenance costs as applications and databases are modified**



As-Is: Securing Sensitive Information

Option 2: Update IBM Product Code

- Multiple user modifications in IBM code
- Changes must be refit as IBM maintenance is applied
- May not satisfy corporate audit requirements not allowing internally developed solutions



To Be: Protecting Sensitive Information in z/TPFDF Files

A database administrator can encrypt data-at-rest in z/TPFDF files and protect sensitive customer information without requiring any application changes.

A database administrator can encrypt data-at-rest in z/TPFDF files and **protect sensitive customer information without requiring any application changes.**

- z/TPFDF data is encrypted when “at-rest”
  - On DASD, in VFA, or in Logical Record Cache (LRC)
- z/TPFDF data is in the clear when used by...
  - Applications through z/TPFDF APIs
  - Operations through z/TPFDF commands
  - Developers through the z/TPFDF interfaces and the z/TPF debugger

A database administrator can encrypt data-at-rest in z/TPFDF files and protect sensitive customer information **without requiring any application changes.**

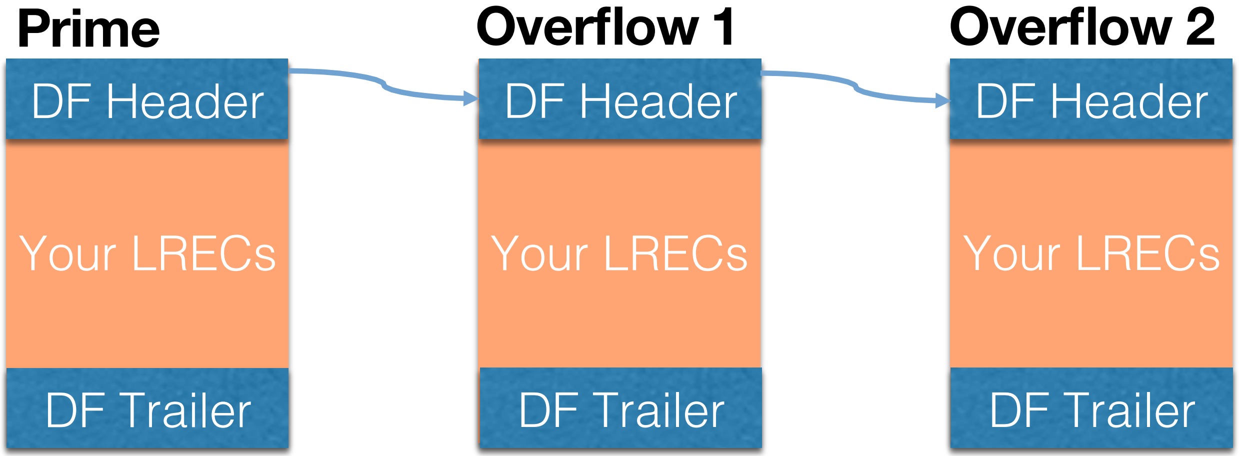
- Encrypt data using AES encryption algorithms in Cipher Block Chaining (CBC) mode
  - AES-128 CBC
  - AES-256 CBC
- Identify accidental and malicious data corruption using data integrity verification
  - Verify data using SHA-256 message digest
  - None (no verification)
- Data is protected by only allowing access through z/TPFDF interfaces
  - z/TPF interfaces (ZDFIL, FIND/FILE APIs) will only see encrypted data

A database administrator can encrypt data-at-rest in z/TPFDF files and protect sensitive customer information without requiring any application changes.

- All z/TPFDF interfaces will automatically encrypt and decrypt z/TPFDF files
  - z/TPFDF programming APIs
  - z/TPFDF commands: ZUDFM and ZFCRU
  - z/TPFDF Recoup
- z/TPFDF encryption is managed through commands and is transparent to applications

As-Is: What is Encrypted?

Without encryption, all z/TPFDF data is in the clear



To-Be: What is Encrypted?

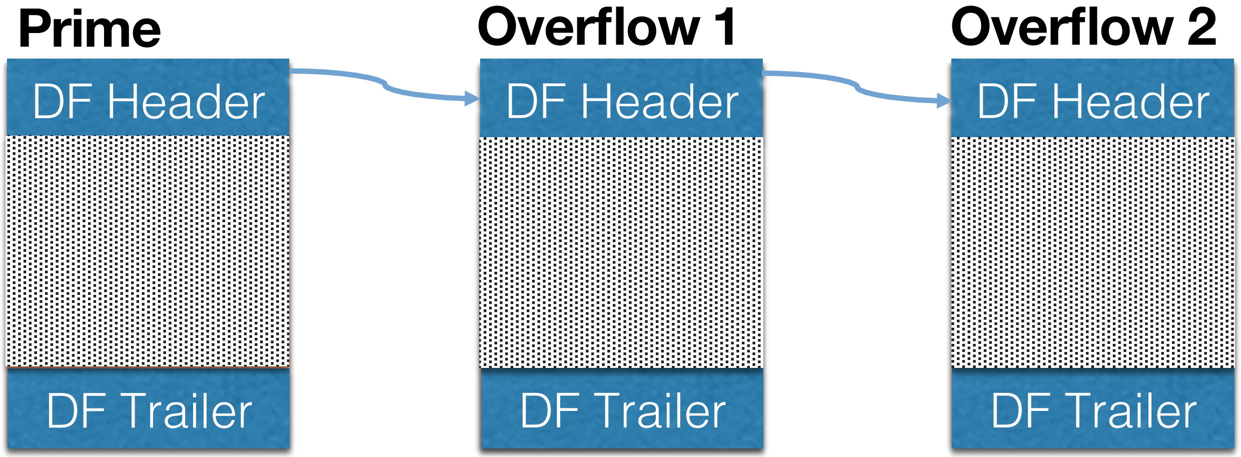
With Encryption:

Encrypted

- Standard data areas (LRECs)
- First block of LLR (MLL)

Not Encrypted

- z/TPFDF standard headers and trailers



Types of z/TPFDF Files Supported

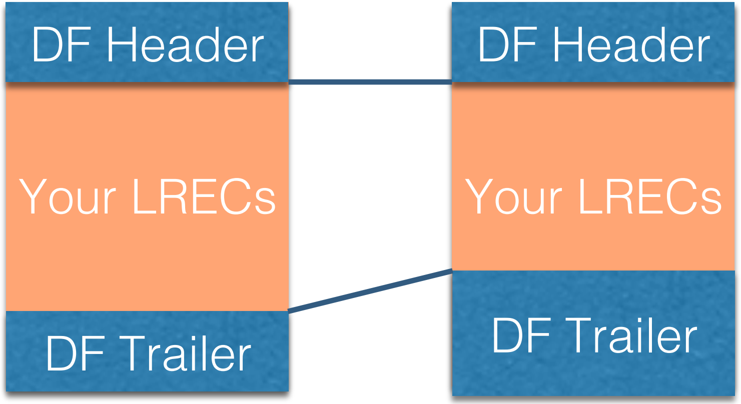
Any z/TPFDF R-type file may be encrypted, except those with the following characteristics

- B+Tree node file
  - NODE=YES is coded on DBDEF
- Uses algorithm #TPFBD0D
- Trailer is not used or contains user data
  - TRS >= 0 is coded on DBDEF

Encrypt existing z/TPFDF files in a few simple steps

Update DBDEF

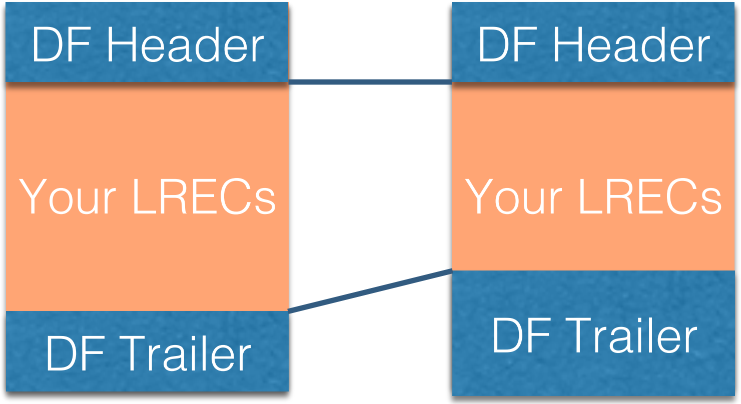
- New parameter on DBDEF to allow encryption
- New subfiles only: Adds encryption controls to trailer in each block
- Reduces maximum size of a single LREC by ~88 bytes



Data is in the clear

Migrate to new trailer format

- Use CRUISE to expand trailer in all subfiles
  - Requires PACK function with new migrate option
  - If LREC exceeds max LREC size:
    - Warn and do not migrate
    - Convert LREC to LLR



Data is in the clear

Define Encryption Keys

- Use z/TPF Symmetric Keystore support to define encryption keys and key names
  - Generate keys using the ZKEYS command
  - Import keys from external keystore

z/TPF Keystore

Enable z/TPFDF Encryption

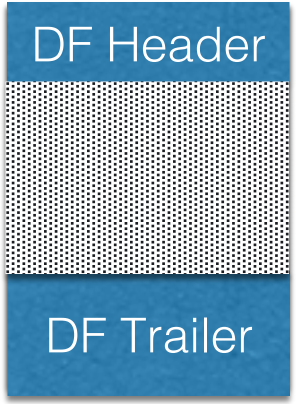
- For each z/TPFDF file, use new ZUDFM ENCRYPT command
  - Define encryption key name
  - Define data integrity verification option
  - Enable encryption
- Individual blocks are encrypted and verified as they are filed by applications

DF Header
DF Trailer

Data is encrypted

Encrypt all blocks

- Use CRUISE with PACK function
  - Pack process will encrypt and file all blocks across selected subfiles
  - Use to make sure all blocks across all subfiles are encrypted
- No downtime required!



Data is encrypted

Potential Future Items

- Encryption of complete LLR
  - Current plan is to only encrypt the Master Large LREC (MLL) block of an LLR
- Node files in a B+Tree
- Clear core blocks before release (RELCC)

z/TPFDF Encryption Summary

- Encrypt data-at-rest in z/TPFDF files
- Encrypt without requiring application changes
- Encrypt without any downtime

Thank you!

Questions or comments?

Trademarks

- IBM, the IBM logo, ibm.com and Rational are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Notes

- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.
- This presentation and the claims outlined in it were reviewed for compliance with US law. Adaptations of these claims for use in other geographies must be reviewed by the local country counsel for compliance with local laws.