z/OS V2.5 IBM Education Assistant

Solution Name: Data Privacy for Diagnostics (DPfD)

Solution Element(s): BCP SVA

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - Apache 2.0.

Objectives

- Things you will learn from this presentation
  - Functional content and benefit
  - How to use/ invoke the new function
  - Migration / Coexistence issues/ concerns
  - List of publications

Overview

- Problem Statement / Needs Addressed
  - z/OS dumps contain diagnostic data critical for problem analysis
    - There may be sensitive data in the storage being captured
  - Clients share data dumps with IBM / vendors / 3rd parties
    - Risk sending sensitive private information accidentally
      - Fail to comply with Privacy Laws and Regulations (ex. GDPR)
        - Hefty fines and loss of credibility
  - Forced to choose between Regulatory Compliance and Serviceability
    - Non-negotiable for many of our clients

Overview

- Impact of sharing sensitive data
  - Irreparable damages to money and reputation

$3.9M

Global average cost of a data breach

The average total cost has increased by **10%** since 2014.

80%

Breaches that contained customer PII

Customer PII is the **most frequently** compromised type of record.

$150

Customer PII average cost per record

Customer PII is also the **costliest** type of record compromised.

Biggest data breach fines in millions of USD

Equifax (575M)

Home Depot(200M)

Uber (148M)

Capital One (80M)

- Hacks enabled by weak security, cover-ups or avoidable mistakes have cost these companies a total of nearly **$1.3B** and counting.

Source: CSO, The biggest data breach fines, penalties and settlements so far, 2020 - bit.ly/33Kt1rk

Overview

- Our Solution
  - z/OS Data Privacy for Diagnostics (DPfD)
  - Implements a two-pronged approach to detect / tag sensitive data
    - Allow z/OS APIs to tag their 64-bit storage with Sensitivity attributes on z15
      - New keyword SENSITIVE=(YES|NO|UNKNOWN)
        - Supported on IARV64/ IARST64/ IARCP64 requests
    - Leverage the z/OS Diagnostics Analyzer
      - Complements the API tagging solution
      - Detects sensitive data in untagged pages
        - Pages tagged sensitive and non-sensitive are skipped
        - Includes a set of built-in identifiers
        - Allows customization to identify sensitive data in one’s environment
        - Written in Java
          - Exploits zIIPs and multi-threading to boost performance

Overview

- Our Solution (continued)
  - Capture storage as usual, along with sensitivity tags
    - Propagate the sensitivity attributes in the dump records
      - no additional impact to dump capture times
    - SVC and Stand-alone dumps (328868) – hbb77b0 to hbb77d0
    - SYSM and Transaction dumps (364824) - hbb77d0
    - Support keyword SENS on GTF parms (hbb77d0)
      - Options are YES|NO|UNK
      - Tag GTF records with Sensitivity Attributes
        - Dump records on GTFPCT are always marked not-sensitive

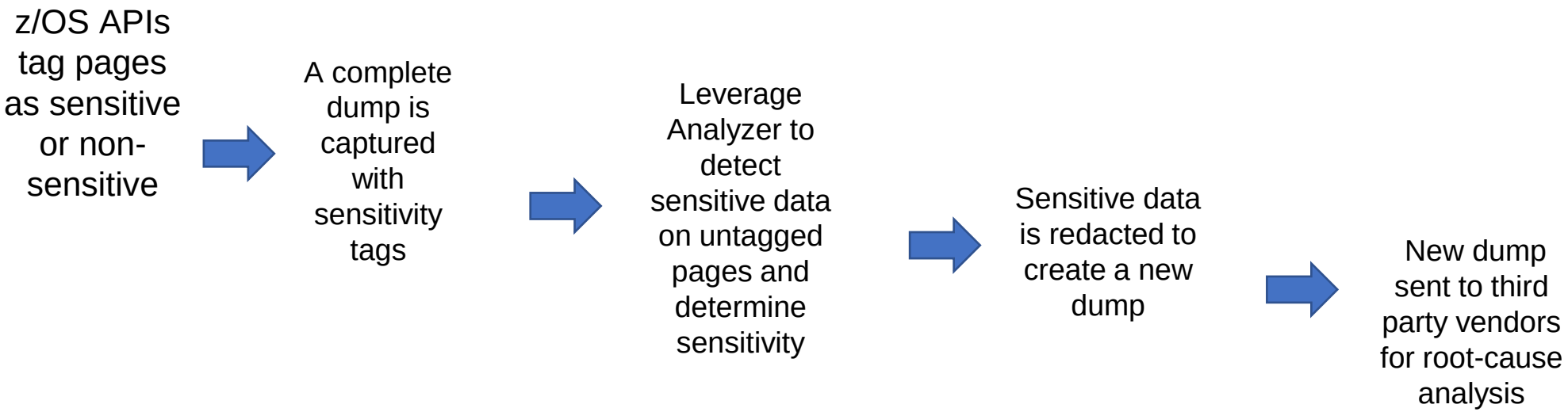
```
/IEFPROC EXEC PGM=AHLGTF,PARM='MODE=EXT,DEBUG=NO,TIME=YES,SENS=YES',  *
//  TIME=1440,REGION=2880K
------
s gtf.VARAN1,,,(MODE=DEFER,SENS=NO,DEBUG=NO)
```

Overview

- Our Solution (continued)
  - z/OS Data Privacy for Diagnostics (DPfD)
    - Post-process the original dump to create a 2nd / redacted dump
      - Utilize the z/OS Diagnostics Analyzer to:
        - Scan, analyze and tag dump records with unknown sensitivity
          - Allows customized detection of sensitive data
        - Redact sensitive data in the dump records
          - Using built-in, custom and dependent identifiers
        - Provide redaction reports
          - List of redacted pages etc.
      - Send the redacted dump for diagnosing the problem

Overview

- Solution workflow



Overview

- Benefits / Value
  - System programmers can share diagnostics material
    - with sensitive data detected and redacted automatically
    - minimal impact to the problem resolution times
  - No need to choose between
    - Diagnostic Capability And Regulatory Compliance
  - Over-redaction is possible and preferred

Usage & Invocation

- On z15 machines
  - All SVC/ Stand-alone/ SYSM and Transaction dumps are redactable
- To post-process a redactable dump
  - File system setup is required (See SYS1.SAMPLIB(BLSDPJIN))
    - Create, initialize and mount the file system to the home directory
    - Shell script provided to create necessary sub-directories
      - **Knowledgebase** – stores ingested knowledge and user feedback
      - **Configuration** – stores configuration files
      - **Reports** – stores generated reports on DPfD functions
        - A subdirectory is created for each dump
          - A subdirectory with each run-number

Usage & Invocation

- IPCS Post-process Panel

```
------------------- IPCS MVS DUMP BATCH JOB OPTION MENU    --------------------
 OPTION  ===>
                                                          *********************
   1  SADUMP     - Prepare stand alone dump for analysis   * USERID  - PURVIP
   2  SVCDUMP    - Prepare SVC dump for analysis           * DATE    - 19/09/24
   3  SYSMDUMP   - Prepare SYSMDUMP for analysis           * JULIAN  - 19.267
   4  SUPPLEMENT - Perform supplementary dump analysis     * TIME    - 01:39
   5  EREP       - Process software data using EREP        * PREFIX  - PURVIP
   6  DPfD       - Data Privacy for Diagnostics            * TERMINAL- 3278
                                                          * PF KEYS - 24
JOB STATEMENT INFORMATION:  (Verify before proceeding)    *********************

  ===> //DPFD JOB MSGCLASS=A,MSGLEVEL=(1,1),REGION=0M,
  ===> //    MEMLIMIT=NOLIMIT
  ===>
  ===>
  ===>
  ===>

Enter END to terminate batch job processing.
```

Usage & Invocation

- IPCS DPfD main panel

```
------------------------- Data Privacy for Diagnostics Request ---------------
COMMAND ===>
Press ENTER to edit parameters, END to terminate without job submission.

REQUESTED FUNCTION ===> ANALYZE   (ANALYZE, REPORT, FEEDBACK, INGEST, EXTRACT)

  ANALYZE  - Analyze the input file using built-in and custom identifiers

  REPORT   - Generate a user friendly report of ANALYZE operation

  FEEDBACK - Provide feedback to fine-tune future DPFD analysis

  INGEST   - Ingest the user provided data

  EXTRACT  - Extract identifier information



 F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=RFIND     F6=MORE
 F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=CURSOR
```

Usage & Invocation

- IPCS DPfD ‘Analyze’ panel

```
Press ENTER to submit the job, END to terminate without job submission.

DATA SET NAME       ===> 'D83DUMP.DYNZOS24.S58.D190911.T221308.SV00006'
NEW DATA SET NAME   ===> 'D83DUMP.DPFD.RED'
TEMP DATA SET/PAT   ===> 'D83DUMP.DPFD.TEMP'
BYPASS DP ANALYSIS ===> N     (Y or N)
REDACTION STRING   ===> !!!!!!!!!!                        (0-32 characters)
NUMBER OF THREADS  ===> 8     (1-8)
ALLOW PAGE LEVEL   ===> Y     (Y or N)
SENSITIVE REPORT   ===> Y     (Y or N)
DPfD HOME DIR      ===> /DPfD
JAVA HOME DIR      ===> /usr/lpp/java/java800/current_64
JAVA OPTIONS       ===> -Xms256m -Xmx4g
JZOS LOAD MODULE   ===> JVMLDM86  (JVMLDMxx, see JZOS Batch Launcher Toolkit)
MIGLIB DATASET     ===> 'SYS1.MIGLIB'
TEMP ALLOC PARMS   ===> storclas(sclarge) dataclas(compress)
EDIT CONFIG FILE?  ===> Y
```

Usage & Invocation

- IPCS – DPfD ‘Analyze’ customize options
  - Number of threads (max 8)
  - Redaction level
    - Page (faster but may over-redact)
      - Token level for below-the-bar storage
    - Token (detailed but can take longer)
  - Redaction string
    - Makes it easier to spot redacted data in dump pages

Usage & Invocation

- New IPCS message at dump initialization
  - Redactable but not post-processed dump

```
IKJ56650I TIME-05:09:44 PM. CPU-00:00:04 SERVICE-394156 SESSION-02:29:07 JANUARY
15,2020
BLS18122I Initialization in progress for
DSNAME('MVSSVA.VARAN1.TWEAKSWO.NOREDACT.S00003')
BLS18124I TITLE=DPFD0011 WITH SUMLIST64
BLS18223I Dump written by z/OS 02.04.00-0 SVC dump - level same as IPCS level
BLS18558I This redactable dump has not been post-processed to protect sensitive data
BLS18222I z/Architecture mode system
BLS18255I Dump Init    Elapsed Time          CPU Time
          Input I/O   00:00:00.507451     00:00:00.010237
          DDIR        00:00:00.044555     00:00:00.021118
```

Usage & Invocation

- New IPCS message at dump initialization
  - Redactable and Post-processed dump

```
IKJ56650I TIME-10:21:06 AM. CPU-00:00:01 SERVICE-154397 SESSION-01:15:51 JANUARY 15,2020
BLS18122I Initialization in progress for DSNAME('MVSSVA.SECURDMP.SADMP.DPA.AFTERE35')
BLS18124I TITLE=SADMP DPFD0001
BLS18223I Dump written by z/OS 02.04.00-0 SADUMP - level same as IPCS level
BLS18557I This redactable dump has been post-processed to protect sensitive data
BLS18222I z/Architecture mode system
BLS18125I CPU(1) STATUS available
BLS18125I CPU(2) STATUS available
BLS18310I Stand alone dump required 00:03 to record to MVSSVA.SECURDMP.SADMP
BLS18255I Dump Init    Elapsed Time          CPU Time
          Input I/O   00:00:01.408455     00:00:00.023984
          DDIR        00:00:00.242923     00:00:00.124712
```

Usage & Invocation

- New message during post-processing
  - Attempt to redact an unsupported dump
    - non-z15 dump

```
" 2021-02-19 13:11:58 INFO PageData:365 - Dump supported : false : 00"
" 2021-02-19 13:11:58 INFO FileProcessor:267 - Header Status : false"
" 2021-02-19 13:11:58 INFO DumpReaderZfile:142 - Going to close : //'D83DUMP.SYSZOS25.ZD00FJH6.SV02922'"
" 2021-02-19 13:11:58 ERROR FileProcessor:103 - The dump version is not supported."
" 2021-02-19 13:11:58 ERROR EntryPoint:257 - Error during processing : "
" com.ibm.irl.data.sdi.SdiException: The dump version is not supported."
```

    - a post-processed dump and Analysis was bypassed

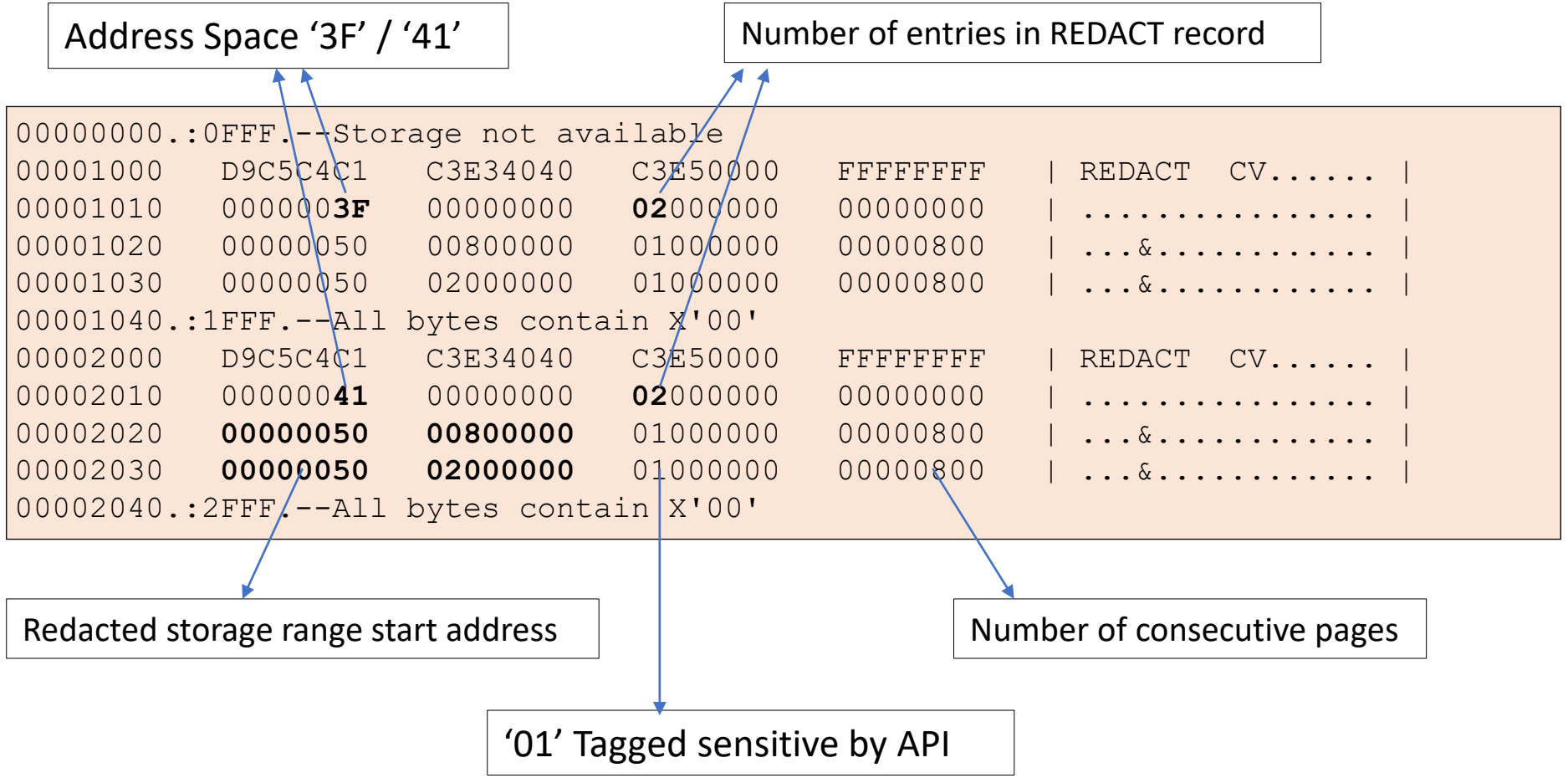
```
16.09.01 JOB08341  $HASP373 E35POSTP STARTED - WLM INIT  - SRVCLASS WLMLONG  - SYS AQTS
16.09.01 JOB08341  IEF403I E35POSTP - STARTED - TIME=16.09.01
16.09.01 JOB08341  +BLS18556I The input data is not eligible for DPfD post processing
16.09.01 JOB08341  -
```

Usage & Invocation

- New IPCS component record BLSREDCT
  - Lists pages tagged sensitive by an API or Analyzer
  - SVC Dump
    - BLSREDCT for API tagged pages is created at the dump write time
    - BLSREDCT for Analyzer tagged pages is created during post-processing
  - Stand-alone dump
    - BLSREDCT is created during post-processing for API and Analyzer tagged pages

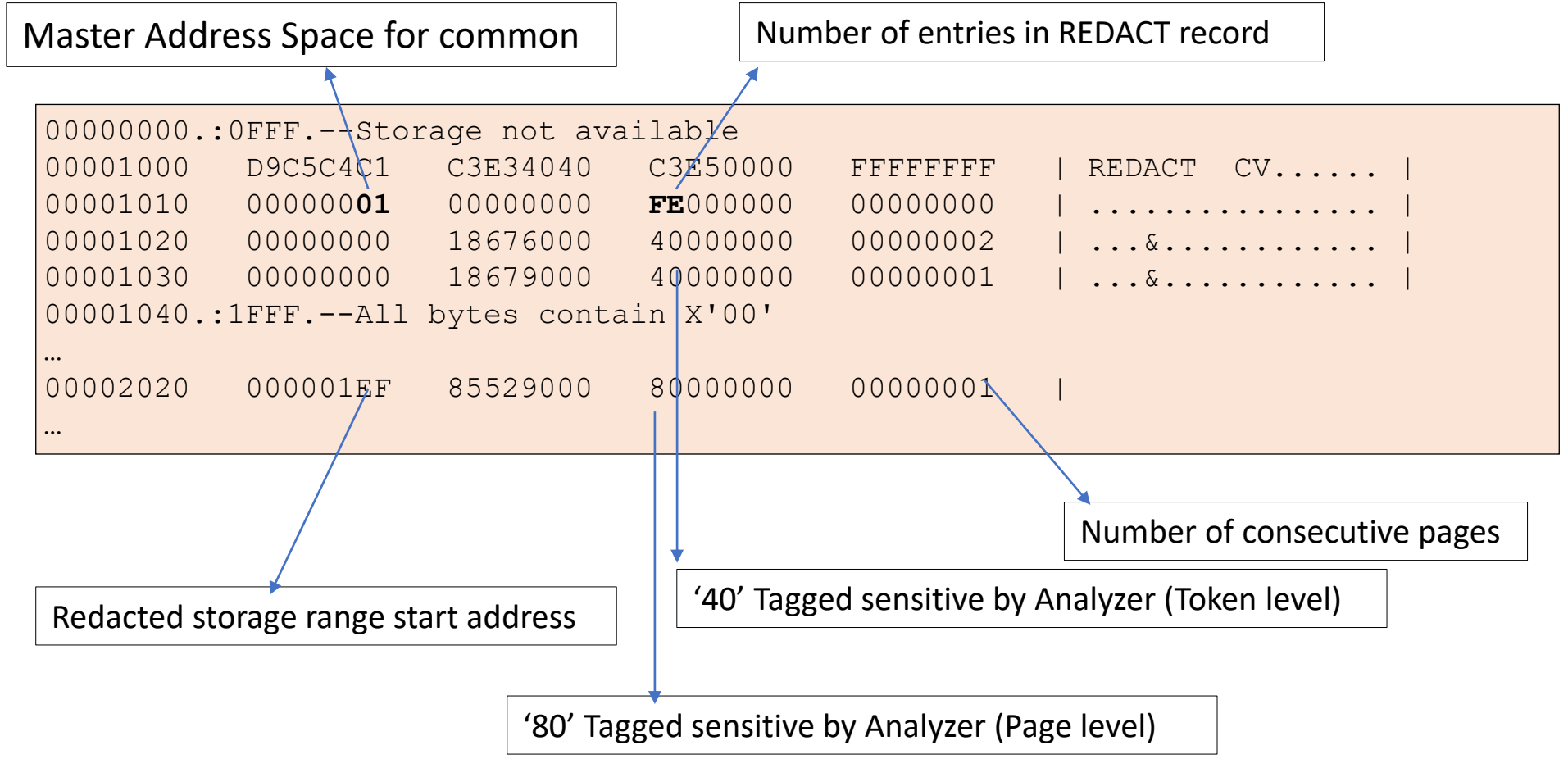
Usage & Invocation

- New IPCS component record BLSREDCT



Usage & Invocation

- New IPCS component record BLSREDCT (continued)



Usage & Invocation

- New IPCS REXX exec
  - BLSXREDR – REXX that reads COMPDATA(BLSREDCT)
    - Lists ranges tagged sensitive
    - Can be invoked from IPCS or TSO
    - Input – dump name, ASID (optional)

Usage & Invocation

- BLSXREDR sample output
  - In TSO: %BLSXREDR 'MVSSVA.DPFD.TESTDUMP'

```
Dump being analyzed: 'MVSSVA.DPFD.TESTDUMP'
.
  00000000_7EBB0000 : 00000000_7EBB0FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_7EBBA000 : 00000000_7EBBAFFF, Redacted by Data Privacy Analysis, partial page(s)
.
Records for ASID 0007
  00000050_0020A000 : 00000050_0020AFFF, Redacted by Data Privacy Analysis, whole page(s)
  00000050_00212000 : 00000050_00213FFF, Redacted by Data Privacy Analysis, whole page(s)
  00000050_00688000 : 00000050_00688FFF, Redacted by Data Privacy Analysis, whole page(s)
  00000050_00878000 : 00000050_00878FFF, Redacted by Data Privacy Analysis, whole page(s)
.
Records for ASID 0006, DSPNAME=IXCDSMEM.
  00000000_00900000 : 00000000_00901FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_01200000 : 00000000_01200FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_01D00000 : 00000000_01D00FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_02400000 : 00000000_02400FFF, Redacted by Data Privacy Analysis, partial page(s)
.
Records for COMPDATA='IARHVSHR'.
  0000040C_FEFB9000 : 0000040C_FEFB9FFF, Redacted by Data Privacy Analysis, whole page(s)
  0000040C_FF015000 : 0000040C_FF015FFF, Redacted by Data Privacy Analysis, whole page(s)
  0000040C_FF01F000 : 0000040C_FF01FFFF, Redacted by Data Privacy Analysis, whole page(s)
  0000040C_FF068000 : 0000040C_FF068FFF, Redacted by Data Privacy Analysis, whole page(s)
  0000040C_FF087000 : 0000040C_FF087FFF, Redacted by Data Privacy Analysis, whole page(s)
```

Usage & Invocation

- BLSXREDR sample output
  - In TSO: %BLSXREDR 'MVSSVA.DPFD.TESTDUMP' A A5

```
Dump being analyzed: 'MVSSVA.DPFD.TESTDUMP'
Records for ASID 00A5
  00000000_00DB7000 : 00000000_00DB8FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_00DC0000 : 00000000_00DC0FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_00DC4000 : 00000000_00DC4FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_00DC6000 : 00000000_00DC8FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_7F266000 : 00000000_7F266FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_7F295000 : 00000000_7F295FFF, Redacted by Data Privacy Analysis, partial page(s)
  00000000_7F2A6000 : 00000000_7F2A6FFF, Redacted by Data Privacy Analysis, partial page(s)
..
  00000010_008FF000 : 00000010_008FFFFF, Redacted by Data Privacy Analysis, whole page(s)
  00000010_00AFC000 : 00000010_00AFCFFF, Redacted by Data Privacy Analysis, whole page(s)
  0000005C_80007000 : 0000005C_80007FFF, Redacted by Data Privacy Analysis, whole page(s)
Records for COMPDATA='IARHVSHR'.
  00000321_00006000 : 00000321_00006FFF, Redacted by Data Privacy Analysis, whole page(s)
  00000321_F8A79000 : 00000321_F8A79FFF, Redacted by Data Privacy Analysis, whole page(s)
  00000321_F8C10000 : 00000321_F8C10FFF, Redacted by Data Privacy Analysis, whole page(s)
```

Usage & Invocation

- IP LIST sample output before and after page-level redaction
  - sensitive ranges in the original dump

```
>> ip list 50_00800000. asid(x'41') len(4096)

LIST 50_00800000. ASID(X'0041') LENGTH(X'1000') AREA
_0800000 LENGTH(X'03B0')==>All bytes contain X'00'
_08003B0. 00D3E8C4 C9C14040 40404040 4040D2C5 |.LYDIA        KE|
_08003C0. D3D3E840 40404040 40404040 4040D74B |LLY           P.|
_08003D0. D64B40C2 D6E740F1 F5F96B40 F3F6F9F4 |O. BOX 159, 3694|
_08003E0. 40D4C1E4 D9C9E240 E2E34B40 40404040 | MAURIS ST.     |
_08003F0. 40404040 4040E2C1 D540D1D6 C1D8E4C3 |      SAN JOAQUC|
_0800400. 60D54040 40404040 40404040 40404040 |-N              |
_0800410. 40404040 4040F0F8 F4F8F340 40404040 |      08483     |
_0800420. 4040F5F1 F5F6F1F8 40F4F6F1 F7F3F640 |  515618 461736 |
_0800430. F7F4F3F1 40F2F1F9 00000000 00000000 |7431 219........|
_0800440 LENGTH(X'0BC0')==>All bytes contain X'00'
```

  - sensitive ranges in the post-processed dump

```
>> ip list 50_00800000. asid(x'41') len(200)

LIST 0050_00800000. ASID(X'0041') LENGTH(X'C8') AREA
_0800000. D9C5C4C1 C3E3C5C4 40C4C1E3 C1000000 |REDACTED DATA....................|
_0800010. 00000000 00000000 00000000 00000000 |................................|
_6B00020 LENGTH(X'A0')==>All bytes contain X'00'
_6B000C0. 00000000 00000000                   |........                        |
```

Usage & Invocation

- IP LIST sample output before and after token-level redaction
  - sensitive ranges in the original dump

```
LIST 0B1A0320. ASID(X'0038') LENGTH(X'64') AREA
0B1A0320. 00000000 00000000 0000C194 81A88140 |.........Amaya |
0B1A0330. 40404040 404040E2 A3859788 8595A296 |       Stephenso|
0B1A0340. 95404040 404040F2 F0F760F4 F9F9F540 |n      207-4995 |
0B1A0350. C58785A2 A381A240 E2A39985 85A34040 |Egestas Street  |
0B1A0360. 40404040 40404040 40404040 404040C4 |               D|
0B1A0370. 85A39996 89A34040 40404040 40404040 |etroit          |
0B1A0380. 40404040                            |                |
```

  - sensitive ranges in the post-processed dump

```
LIST 0B1A0320. ASID(X'0038') LENGTH(X'64') AREA
0B1A0320. 00000000 00000000 00005A5A 5A5A5A5A |.........!!!!!!|
0B1A0330 LENGTH(X'40')==>All bytes contain X'5A', EBCDIC C'!'
0B1A0370. 5A5A5A5A 5A5A4040 40404040 40404040 |!!!!!!          |
0B1A0380. 40404040                            |                |
```

Interactions & Dependencies

- Software Dependencies
  - No
- Hardware Dependencies
  - z15
- Exploiters
  - Db2, IMS, VSAM, various DFSMS components
  - ZFS (z/OS V2.5 only)

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Sysplex must be at the new z/OS level: No
- Fix Category: IBM.Function.DataPrivacyForDiagnostics
- List of toleration/coexistence APARs/PTFs.
  - Storage Manager (API-1) OA57633 (UJ00688, UJ00699)
  - Storage Manager (API-2) OA58289 (UJ03895, UJ03896)
  - Storage Manager (API-2 PE) OA60373 (UJ04600, UJ04601)
  - Service Aids Support OA57570 (UJ00714, UJ00715)
  - Service Aids Support OA58114 (UJ04756, UJ04586)
  - Basic Access Methods OA58712 (UJ01664, UJ01665)
  - Object Access Method OA58431 (UJ01359, UJ01360)
  - Db2 PH15940 (UJ65280)
  - IMS PH14059 (UJ65556)
  - VSAM OA58730 (UJ04647,UJ04649)

.

Upgrade & Coexistence Considerations

- List anything that doesn't work the same anymore
  - No change. Original dumps before DPfD post-processing are same as before, except that the dump records contain sensitivity attributes of the storage captured.
- Coexistence applies to lower-level systems which coexist (share resources) with latest z/OS systems.
  - Function available on v2r3 and above.

Installation & Configuration

- Are any APARs or PTFs needed for enablement? Yes, see the slide on PTFs
- What jobs need to be run? See slides on Post-processing
- What hardware configuration is required? z15
- What PARMLIB statements or members are needed? None
- Are any other system programmer procedures required? N/A
- Are there any planning considerations? N/A
- Are any special web deliverables needed? N/A
- Does installation change any system defaults? no

Summary

- z/OS Data privacy for Diagnostics
  - Available on z15 machines
  - Designed and developed to help clients comply with Privacy policies / regulations
    - Without sacrificing diagnostic capabilities
  - Creates a second, redacted dump by post-processing the original dump
    - By removing/redacting sensitive data
  - Allows APIs to tag their known 64-bit storage with Sensitivity attributes
    - 31-bit storage is subjected to token-level redaction by the z/OS Diagnostics Analyzer
      - Except various system areas (NUC, LPA, system trace buffers which are considered not-sensitive)
  - Optional post-processing to secure sensitive data
    - Ingests the sensitive data/ data patterns
    - Exploits parallelism
    - Scans, detects and tags sensitive data in untagged dump records
      - Using Built-in / Custom / dependent identifiers
    - Allows to fine-tune redaction through the Feedback function
  - Over-redaction is possible and preferred
  - Only redactable and unredacted dumps can be post-processed.

Appendix

- Publications:
  - z/OS MVS IPCS Commands (SA23138200)
  - z/OS MVS IPCS Customization (SA23138300)
  - z/OS MVS IPCS Messages (SA2275900)
  - z/OS MVS IPCS User’s Guide (SA23138400)
  - z/OS Version 2 Release 5 of MVS System Commands (SA38066600)
  - z/OS MVS Diagnosis: Tools and Service Aids (GA32090500)