z/TPF V1.1

TPF Users Group Spring 2008

Title: Nondisplayable ECB Storage

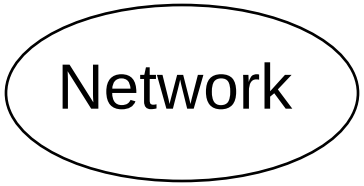
z/TPF APAR PJ31995

Name: Michael Shershin
Venue: Main Tent

AIM Enterprise Platform Software
IBM z/Transaction Processing Facility Enterprise Edition 1.1.0

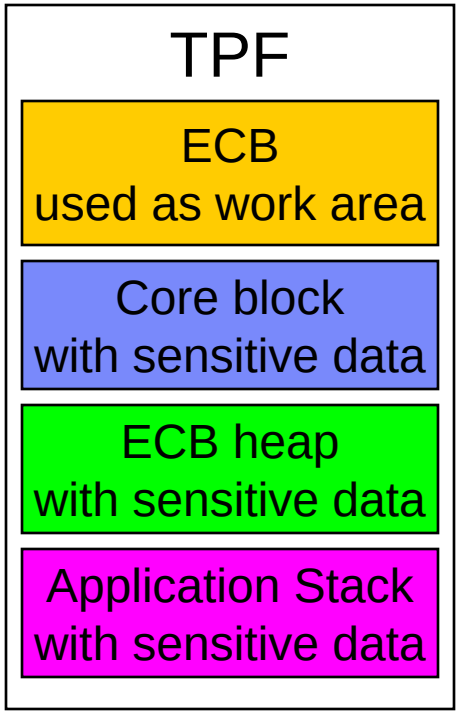
Securing Data

Data in flight



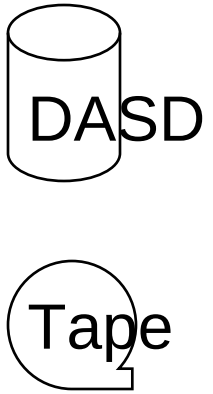
Sensitive data encrypted when transmitted over the network.

Data in use



Sensitive data needs to be secure when it is being used.

Data at rest



Sensitive data encrypted when saved on DASD or on tape.

What is Nondisplayable ECB Storage?

- **A method to secure sensitive data in use**
- **Prevent areas of working storage from being displayed**
  - Dumps will not display data
    - Dumps will include a list of nondisplayable areas
  - Commands like ZDCOR / ZDDCA will not display data
  - Debugger will not display data
  - Data will be displayed as ********

Dump example

List of Nondisplayable areas in the dump

ECB SVA ADDRESS	ECB NONDISPLAYABLE STORAGE EVA	NONDISPLAYABLE STORAGE SVA	LENGTH
0B995000	000000000E10EFF0	0000000421319FF0	00000010

Actual dump data

```
000000000E10EFD8  00000000  00000000  00000000  0E1F0540  ..........
000000000E10EFE8  00000000  0000000D  ********  ********  ..........
000000000E10EFF8  ********  ********  10111213  14151617  ..........
000000000E10F008  18191A1B  1C1D1E1F  20212223  24252627  ..........
```

ZDCOR example

Displayable Storage

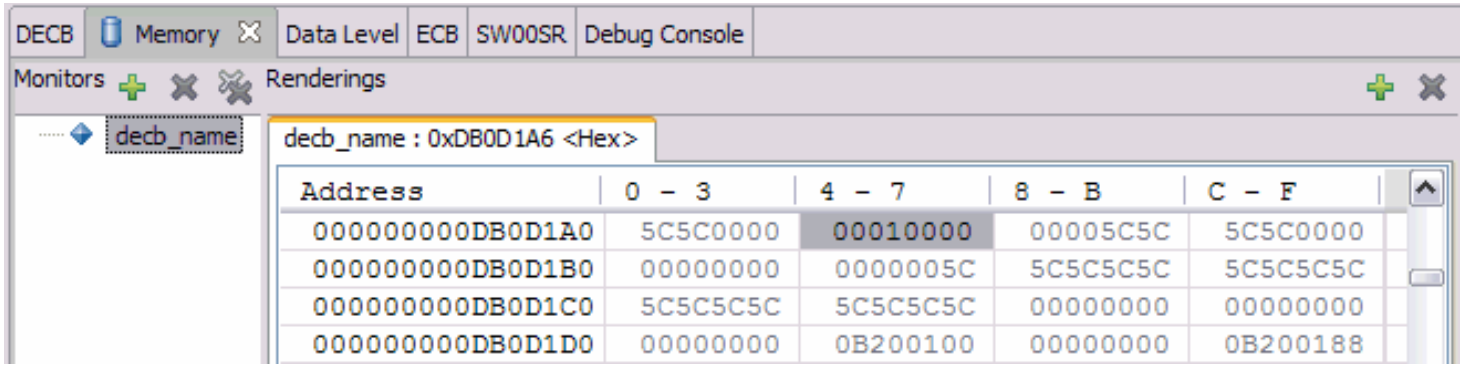
```
==> ZDCOR 0000000420D2CFE0.30
CSMP0097I 16.24.07 CPU-B SS-BSS  SSU-HPN  IS-01 _
DCOR0010I 16.24.07 BEGIN DISPLAY
0000000420D2CFE0- 00000000 0E1F0540 00000000 0000000E .......  ........
0000000420D2CFF0- 00010203 04050607 08090A0B 0C0D0E0F ........ ........
0000000420D2D000- 10111213 14151617 18191A1B 1C1D1E1F ........ ........
END OF DISPLAY - ZEROED LINES NOT DISPLAYED+
```

Nondisplayable Storage

```
==> ZDCOR 0000000420D2CFE0.30
CSMP0097I 16.24.32 CPU-B SS-BSS  SSU-HPN  IS-01 _
DCOR0010I 16.24.32 BEGIN DISPLAY
0000000420D2CFE0- 00000000 0E1F0540 00000000 0000000E .......  ........
0000000420D2CFF0- ******** ******** ******** ******** ........ ........
0000000420D2D000- 10111213 14151617 18191A1B 1C1D1E1F ........ ........
END OF DISPLAY - ZEROED LINES NOT DISPLAYED+
```

Debugger

- **Nondisplayable areas of storage will be shown as**
  - x’5C’ in hexadecimal displays
  - c’*’ is character displays



Nondisplayable ECB Storage APIs

- **Assembler**
  - NDSPC FUNCTION=MARK,AREA=(addr, length)
  - NDSPC FUNCTION=UNMARK,AREA=(addr, length)
- **C**
  - tpf_ndsp_mark(void *address, int length)
  - tpf_ndsp_unmark(void *address, int length)

Areas of storage that can be nondisplayable

- **Only ECB unique areas are allowed**
  - ECB - CE1WKA, CE1WKB, user areas
  - Core blocks in ECB private area
  - ECB Heap
  - Application stack
  - Static area (the program)
  - DECB

Nondisplayable data passed to created ECBs

- **Data passed to created ECBs will maintain nondisplayable properties**
  - CREMC / CREDC / CREXC
    - Data passed in EBW area
  - CREEC / SWISC CREATE
    - Data passed in EBW area
    - Core block passed
  - CRETC
    - Core block passed
  - fork()
    - ECB heap
    - Application stack
    - Static

How to use Nondisplayable ECB Storage

- **Decrypt sensitive data**
  - Sensitive data is encrypted in a core block, heap, or stack.
  - Call NDSPC FUNCTION=MARK to not display an area of storage.
  - Decrypt the sensitive data into the marked storage.
  - Work with the data.

How to use Nondisplayable ECB Storage

- **Encrypt sensitive data**
  - Storage containing sensitive data is marked as nondisplayable
  - Encrypt the sensitive data in the marked storage.
  - Call NDSPC FUNCTION=UNMARK to allow display of this area of storage.
  - Put data where it is supposed to be
    - File to DASD
    - Write to tape
    - Send across network

What happens when Nondisplayable Storage is no longer needed?

- **NDSPC FUNCTION=UNMARK**
  - Data can be displayed.
  - Previous nondisplayable data is not touched. It will not be zeroed.
- **ECB EXITC without doing unmark**
  - Nondisplayable data will be zeroed.
- **RELCC without doing unmark**
  - Nondisplayable data will be zeroed.
- **free() without doing unmark**
  - Nondisplayable data will be zeroed.

What happens when Nondisplayable Storage is no longer needed (continued)?

- **realloc()**
  - If heap is relocated, the new area inherits the nondisplayable properties from the previous area.
  - If heap is relocated, nondisplayable data in old area is zeroed.
- **CREEC / SWISC CREATE / CRETC passing core block to new ECB**
  - When a create-type macro is executed and a core block is passed to the created ECB, there are two actions which happen:
    - In the newly created ECB, nondisplayable properties are maintained in the core block that was passed.
    - In the ECB that executed the create type macro, a core block being passed is treated like a RELCC. Nondisplayable areas are zeroed when the core block is released.

Controls

- **SIP CONFIG macro**
  - NDSP=ENABLE/DISABLE
    - NDSP=ENABLE hides data
    - NDSP=DISABLE allows nondisplayable data to be viewed.
    - Default is NDSP=ENABLE.
- **Command**
  - ZMNDS ENABLE
    - NDSPC FUNCTION=MARK will prevent data from being displayed.
  - ZMNDS DISABLE
    - NDSPC FUNCTION=MARK can still be executed. However, data can be displayed.
    - Intended for test systems that do not use real data.
  - ZMNDS DISPLAY

Questions ???

Trademarks

- IBM is a trademarks of International Business Machines Corporation in the United States, other countries, or both.
- Other company, product, or service names may be trademarks or service marks of others.

- 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.