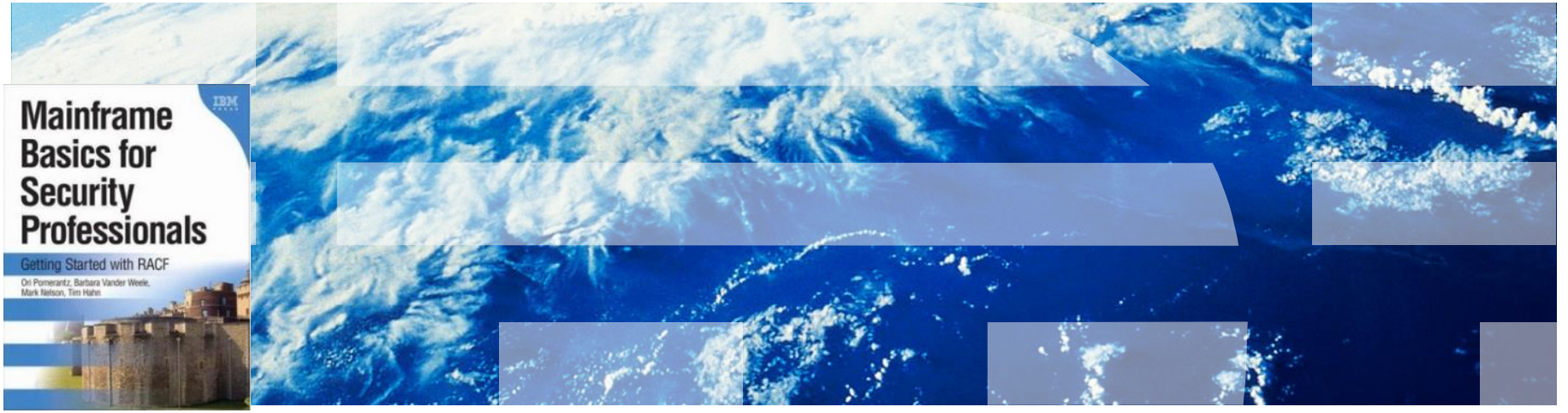
A Fresh Look at Erase-on-Scratch

Kentucky-Ohio-Indiana RACF® Users Group
10 May, 2018

Mark Nelson, CISSLP, CSSLP®
z/OS Security Server (RACF) Design and Development
IBM® Poughkeepsie
markan@us.ibm.com



A Fresh Look at Erase-on-Scratch

- **What do you need to do to read residual data on a z/OS system that has not enabled erase-on-scratch?**
  - Authorized code that reads beyond the end-of-file (EOF) marker?
  - Complicated high-level language code with complicated file declarations?
  - Assembler code?
  - Common utilities?
  - Answer: Any of the above!

- **What is erase-on-scratch?**
  - A RACF and DFSMSdfp facility which causes the overwriting of the space occupied by a data set which has been deleted or for which space is being released (sometimes referred to as “scratched”)

A Fresh Look at Erase-on-Scratch…

- **The SETROPTS options which control erase-on-scratch are:**
  - **SETROPTS ERASE(ALL)**
    - Instructs DFSMSdfp to erase all scratched data sets, *including temporary data sets*, regardless of the erasure indicator in the data set profile
  - **SETROPTS ERASE(seclevel-name)**
    - Instructs DFSMSdfp to erase all scratched data sets that have a security level equal to or greater than seclevel-name
  - **SETROPTS SETROPTS ERASE or ERASE(NOSECLEVEL)**
    - RACF instructs DFSMSdfp to erase a scratched data set if the erasure indicator in the data set profile is on
  - **SETROPTS NOERASE**
    - No erase-on-scratch processing is to be performed, even if the data set erasure indicator is on in the data set profile
  - **Caution:** SETROPTS LIST can displays the ERASURE status over multiple lines:

```
ERASE-ON-SCRATCH IS ACTIVE, CURRENT OPTIONS:
   ERASE-ON-SCRATCH BY SECURITY LEVEL IS INACTIVE
                      vs.
ERASE-ON-SCRATCH IS ACTIVE, CURRENT OPTIONS:
   ERASE-ON-SCRATCH FOR ALL DATA SETS IS IN EFFECT
   ERASE-ON-SCRATCH BY SECURITY LEVEL IS INACTIVE
```

A Fresh Look at Erase-on-Scratch…

- **All settings other than SETROPTS ERASE(ALL) and SETROPTS NOERASE look at the data set erasure status of the data set. This can be set by:**
  - **The RACF data set profile:** `ALTDSD 'MARKN.*' ERASE` causes RACF to instruct DFSMSdfp to "overwrite" the DASD storage occupied by a data set which is being deleted or is having its storage released for data sets covered by this profile
  - **JCL:** CROPS=RCK on the AMP keyword on a DD statement for a VSAM data set or SECMODEL= on a DD statement for an SMS-managed data set

- **Who is using erase-on-scratch?**
  - The April 2013 RSH Consulting survey revealed:
    - ERASE ALL: 13.6%
    - ERASE SECLEVEL: 2.3%
    - ERASE NOSECLEVEL: 22.7%
    - NOERASE: 61.4%

- **What is preventing the more widespread adoption of erase-on-scratch?**
  - Fear of performance impacts!

A Fresh Look at Erase-on-Scratch…

- **There have been considerable changes since erase-on-scratch was introduced in RACF 1.7:**
  - Faster disk drives, control units, and paths to devices
  - Multiple paths to devices
  - Virtualization of devices
  - Data Space Release (DDSR) (which is no longer available)
  - Locate record with erase (LRE)
  - **Up to 255 tracks in a single channel program (z/OS V2R1)**
  - **Up to 12,240 tracks in a single channel program (z/OS V2R2)**

A Fresh Look at Erase-on-Scratch…

- **Frank Kyne performed erase-on-scratch testing that is documented in Cheryl Watson's "TUNING Letter - 2014 No. 1":**
  - Allocated data sets of 1, 100, 255, 25600, and 63000 tracks
  - Ran a separate job to delete each data set, varying erase-on-scratch on and off, on z/OS V1R13 and z/OS V2R1
- **Frank's results:**
  - Small reduction in elapsed time and EXCP counts for the smaller data set sizes (1, 100, 255)
  - Large reduction in elapsed time and EXCP counts for the larger data sets
    - For the 63,000 track data set, EXCPs dropped from 63,007 to 263
    - Elapsed times decrease between 1/3 and 2/3
- **Remember that z/OS V2R2 increases the upper limit on the number of tracks erased in a single CCW to 12,240 (from 255)!**

A Fresh Look at Erase-on-Scratch…

- **One thing to look for before enabling SETROPTS ERASE(ALL):**

  - **If you are using PPRC (“Peer to Peer Remote Copy”), IBM’s synchronous data mirroring technology, have you installed APAR OA46511?**

    - Introduced a new DEVSUPxx keyword (**EOSV2**) to allow the erasure of up to the z/OS maximum for tracks in a single channel program if the PPRC primary and backup data sets

    - Devices must be at a current microcode level

      DS8100/DS8300: 64.36.89.0

      DS8700: 76.31.70.0

      DS8800: 86.31.86.0

A Fresh Look at Erase-on-Scratch…

- **Once you are on any supported release of z/OS, perhaps it's time to revisit erase-on-scratch!**

A Fresh Look at Erase-on-Scratch

Kentucky-Ohio-Indiana RACF® Users Group
10 May, 2018

Mark Nelson, CISSLP, CSSLP®
z/OS Security Server (RACF) Design and Development
IBM® Poughkeepsie
markan@us.ibm.com