A Mainframe Security Rosetta Stone

Translating Concepts and Commands Between Mainframe Security Products

Reg Harbeck, MA, IBM CHAMPION for Z

Chief Strategist

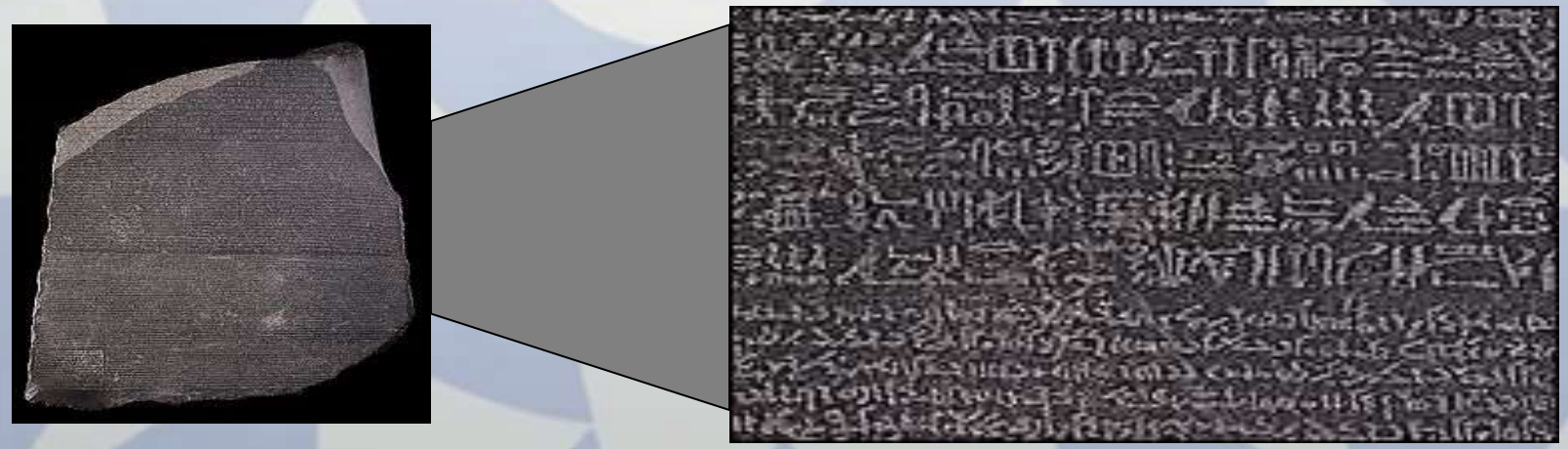
Mainframe Analytics ltd.

Agenda

- What's a Rosetta stone?
- About this session
- Introducing the z/OS security packages
  - IBM RACF
  - CA ACF2
  - CA TSS
- Mapping the concepts and commands
- Where to find out more
- Q&A

What's a Rosetta Stone?

- The Rosetta Stone is a stone with writing on it in two languages (Egyptian and Greek), using three scripts (hieroglyphic, demotic and Greek)
- Knowing one enabled learning the other two



(See http://www.ancientegypt.co.uk/writing/rosetta.html for more.)

What This Presentation is *Not*

- A Roadmap for converting between mainframe security products
- A Sales Pitch for any specific security product(s)
- Exhaustive or highly-detailed or expert-level
- Perfectly unbiased (but I'll try)

The Goal of this Session

- To build on your knowledge of one (or more) mainframe security products to introduce the other(s)
- To review the basic concepts of mainframe security
- To show how each security package maps to them from a high-level
- To review some sample constructs and commands and how they map between products
- To increase appreciation of mainframe security in general

Introducing the z/OS Security Packages

- IBM RACF® (RACF)
- CA ACF2™ (ACF2)
- CA Top Secret® (TSS)
- All use SAF
  - System Authorization Facility
  - Invoked for security access checks, passes the request along to the appropriate security system
- All have Security Databases ("Directories")
  - Not X.500 directories but highly-efficient legacy systems
  - Now accessible from X.500 via LDAP

RACF

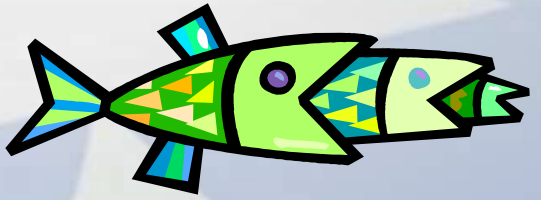
- Resource Access Control Facility
- The original mainframe security system (1976)
  - Unless you count UADS, the PASSWORD file and dataset protection bits, DFHSNT…
- "Profile Oriented"
- Uses dataset protection bits with discrete profiles; deleted with protected object
- Generic profiles more policy-based, not attached to objects secured
- IDs are called "user IDs"
- Commands are like other TSO commands

RACF

- Four kinds of security profiles:
  - User
  - Group
    - Each user belongs to at least one Group
  - Dataset
  - General Resource
    - Both Dataset and General Resource profiles may be Discrete or Generic, and both have Access Lists
- Security database
  - A non-VSAM single extent data set

ACF2

- "Access Control Facility 2" aka "ACF2"
  - Developed by SKK (Schrager, Klemens and Krueger) in 1978 and marketed by Cambridge
  - Cambridge was acquired by UCCEL, who was acquired by CA in 1987, and Broadcom in 2018
- "Resource Oriented"
  - Resources are defined and permitted through rules
- IDs are called "LIDs" (for Logon IDs)
  - Are substrings of UID strings which are used for access determination
- Commands issued directly to ACF2 after "ACF" command, and then a set command



ACF2

- UID (user identification) String:
  - 1-24 character long "pseudo field" constructed of logonid record fields such as department, location, job function and logonid
  - Allows for grouping of users
  - Often contains user-defined fields
  - Allows grouping in access rules
  - Multi-valued Logonid fields-allow multiple views of a single UID
  - Example: @UID LOC, DIV, DEPT, JOBF, LID

    CH F OP SCH TLC492

LOC = Chicago

DIV = Finance & Data Processing

DEPT = Operations

JOBF = Scheduler

LID = TLC492

ACF2

- Rules:

```
$KEY(SYS1)
BRODCAST  UID(CHFSPSYS) R(A) W(A) A(L) E(A)
BRODCAST  UID(*) R(A) W(A)
PARMLIB   UID(CHFSPSYS) R(A) W(A) A(L) E(A)
PARMLIB   UID(*)
PROCLIB   UID(CHFSPSYS) R(A) W(A) A(L) E(A)
```

- Edited, Compiled, Optionally Decompiled
- Default deny
- Eg. SYS1.PARMLIB: Chicago (CH) Finance & DP (F) Systems Programming (SP) SYSPROG (SYS) = Read(Allow), Write(Allow), Alter(Log but Allow), Execute(Allow)

ACF2

- New Feature: X-ROL Records
  - "Cross-reference role group"
  - Allow for RBAC (Role-Based Access Control)
  - Takes the place of UID String in access control
  - Can have roles grouped inside other roles!
  - ROLE(…) statement in rules used in place of UID(…)

ACF2

- Three VSAM key-sequenced data sets
  - Logonid database
    - One record per logonid
    - Central source for most user data*
      - *Other user data on Infostorage Profile records
  - Rule database
    - Contains all data set access rules
  - Infostorage database – includes the following records:
    - GSO (global system options)
    - Resource rules (all non-data-set access rules)
    - XREF (cross-reference records), X-ROL, etc.
    - SCOPE (limit the authority a specially privileged user has)
    - SHIFT (define periods of time when access is permitted or prevented)
    - PROFILES (security information extracted by SAF RACROUTE=EXTRACT)

Top Secret

- "Top Secret Security" aka "TSS"
- Developed by CGA Software Products Group in 1981
- Acquired by CA in 1985, then Broadcom in 2018

Top Secret

- Security database: one file (as of version 16, VSAM)
- IDs are called "ACIDs" (pronounced **ay**-sids, for ACcessor IDs)
- Tree Structured, "ACID Oriented"
  - Everything (including ACIDs) owned by someone
  - MSCA (Master Security Control ACID) is at the top of the tree
- Resources "owned" and "permitted"
  - By/to ACIDs, Zones, Divisions, Departments, PROFILEs and "ALL Record"
- PROFILEs are a natural form of RBAC
- Uses FACILITYs for anything you can logon to
- Commands issued under TSO are all "TSS " commands

Top Secret

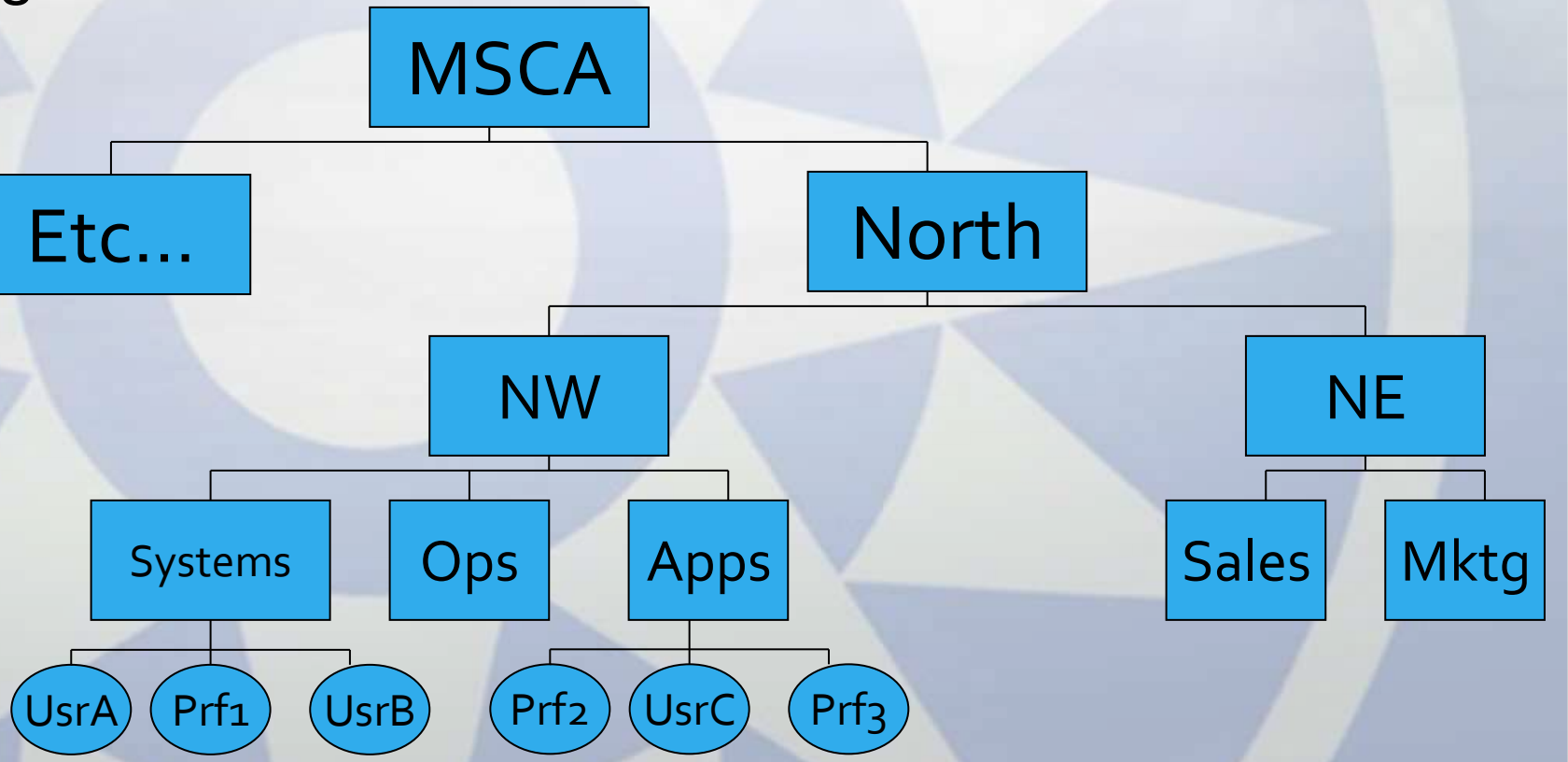
- Hierarchical organization

Zone

Division

Department

Users + Profiles



Defining IDs

- RACF:

ADDUSER *user_id* DFLTGRP(*group*) PASSWORD(*pwd*)

- ACF2:

SET LID

INSERT *logonid* PASSWORD(*pwd*)

- TSS:

TSS CREATE(*accessorid*) DEPARTMENT(*dept*) PASSWORD(*pwd*)

Controlling System Entry

- Batch
  - RACF:
    - Once:
      - `SETROPTS JES(BATCHALLRACF)` forces all BATCH users to be defined to RACF
      - `SETROPTS CLASSACT(JESJOBS)`

    `PERMIT SUBMIT.`*`node.job.userid`* `CLASS(JESJOBS) ID(`*`userid`*`) ACCESS(READ)`
  - ACF2:
    - Once:
      - Specify the JOBCK option of the GSO OPTS record

    `SET LID`

    `CHANGE` *`logonid`* `JOB`
  - TSS:

    `TSS ADDTO(`*`acid`*`) FACILITY(BATCH)`

Controlling System Entry

- TSO
  - Master Catalog Alias, ~~SYS1.UADS~~
  - RACF:

    ```
    ALTUSER userid TSO(ACCTNUM(accnum) PROC(logonproc))
    ```

  - ACF2:

    ```
    SET LID
    CHANGE logonid TSO
    ```

  - TSS:

    ```
    TSS ADDTO(acid) FACILITY(TSO)
    ```

Controlling System Entry

- CICS
  - RACF:

    ```
    ALTUSER userid CICS(OPCLASS(opclass) OPIDENT(opid))
    ```

  - ACF2:

    ```
    SET LID
    CHANGE logonid CICS CICSCL(opclass) CICSID(opid)
    ```

  - TSS:

    ```
    TSS ADDTO(acid) FACILITY(CICS) OPCLASS(opclass) OPIDENT(opid)
    ```

Revoking/Suspending Accounts

- RACF:

  `ALTUSER` *`userid`* `REVOKE`

- ACF2:

  `SET LID`

  `CHANGE` *`logonid`* `SUSPEND`

- TSS:

  `TSS ADDTO(`*`acid`*`) SUSPEND`

Access

- Defining Security for Datasets
  - RACF:
    - Discrete profile:

      ```
      ADDSD 'dsname'
      ```

    - Generic profile:

      ```
      ADDSD 'dsname-incl-generic-char'
      ```

    - **or**

      ```
      ADDSD 'dsname' GENERIC
      ```

  - ACF2:

    ```
    $KEY(high-level-qualifier)
     dsname-extent UID(pattern-for-UIDs) accesses
    ```

  - TSS:

    ```
    TSS ADDTO(acid) DSNAME(dsname-prefix)
    ```

Access

- Permitting Access to Datasets
  - RACF permits access to the names of existing profiles:

    `PERMIT 'profile-name' ID(userid) ACCESS(access)`
  - ACF2 permit is the same as the definition of access:

    `$KEY(high-level-qualifier)`

    `dsname-extent UID(pattern-for-UIDs) accesses`
  - TSS permit is any string of characters beginning with the owned prefix:

    `TSS PERMIT(acid) DSNAME(dsname) ACCESS(access)`

Revoking Access

- Revoking Access from Datasets
  - RACF deletes a permission to a specific named profile:

    `PERMIT 'profile-name' ID(userid) DELETE`
  - ACF2 removes or modifies the line that specifies the access:

    `$KEY(high-level-qualifier)`

    ~~`dsname-extent UID(pattern-for-UIDs) accesses`~~
  - TSS revokes the specific permission:

    `TSS REVOKE(acid) DSNAME(dsname) [ACCESS(access)]`

Universal Access

- Permitting Resource (e.g. Dataset) Access to "Everyone"
  - RACF defines UACC when profile defined:

    ```
    ADDSD 'dsname' UACC(access)
    ```

  - ACF2 drops down to the bottom of the ruleset if nothing more specific found:

    ```
    $KEY(high-level-qualifier)
    . . . various rules . . .
    dsname-extent UID(-) accesses
    - accesses
    ```

  - TSS adds it to the ALL record:

    ```
    TSS PERMIT(ALL) DSNAME(dsname) ACCESS(access)
    ```

Access Permissions: RACF

NONE

- No one can access

READ

- Only Read

UPDATE

- Read and Update

CONTROL

- VSAM only, but imples UPDATE in non-VSAM

ALTER

- Read, Update, Delete, Rename, Move

Access Permissions: ACF2

READ – is read only

ALLOCATE – is allocate only

- DELETE
- CREATE
- RENAME

READ implies EXECUTE

- EXECUTE can be given without READ

WRITE – is write only

EXECUTE – is execute only

Note: Each privilege in CA ACF2 must be given independently
E.g. WRITE does not give READ

Access Permissions: TSS

ALL

- Data set can be accessed in any way

UPDATE

- Data set can be updated; READ and WRITE access is implied

READ

- Data sets can be read (opened for input); the default. READ implies FETCH

WRITE

- Data can only be written into the data set (opened for output)

...

Access Permissions: TSS cont'd

CREATE

- Data set can be created

FETCH

- Programs from the data set (library) can only be executed, not read

SCRATCH

- Data set can be scratched

CONTROL

- VSAM data set can be used for control interval update processing

NONE

- Data set can't be used in any way

Access: Wild Card Characters and Masking

- RACF:
  - % (percent) – Any single character
  - * (asterisk) – Any number of characters in the qualifier (between dots)
    - NB: sometimes * is a stand-alone parameter, not a wild card character
  - ** (two stars) – Any number of characters and qualifiers but alone after "." – use at end of prefix
  - &RACUID and &RACGPID – the user id and current connect group id of the user requesting access
- ACF2:
  - * (asterix) – Any single character
  - – (dash) – Any number of characters (and qualifiers) – use only immediately before "." or at end of permission as prefix
    - "*-." is any one-or-more-character value ending with a "." but "-*." looks for a "-" character at the beginning
  - &LID – The LID of the user requesting access
- TSS:
  - % (percent) – The ACID of the user requesting access
  - + (plus) – Any single character
  - * (splat) – 0-8 characters (including dots)
  - – (dash) – 0-24 characters (including dots)
  - Everything is a prefix (except in select non-dataset resources)

Access

- Grouping Access
  - RACF:

    CONNECT *userid* GROUP(*group*)
  - ACF2:

    SET LID

    CHANGE *logonid* DEPT(*dept*)

  or…

    SET X(ROL)

    INSERT *roleid* ROLE INCLUDE(*lgnid-*) exclude(*logonid1*,*logonid2*)
  - TSS:

    TSS ADDTO(*acid*) PROFILE(*profilename*)

Passwords

- Changing a Password
  - RACF:

    `PASSWORD PASSWORD(newpwd) USER(userid)`
  - ACF2:

    `SET LID`

    `CHANGE logonid PASSWORD(newpwd)`
  - TSS:

    `TSS REPLACE(acid) PASSWORD(newpwd)`

Displaying User Security Settings

- Listing a user's information
  - RACF:

    `LISTUSER (userid)`

    `LISTUSER (userid1,userid2,*)`
  - ACF2:

    `SET LID`

    `LIST logonid`

    `LIST LIKE(logonid-mask)`
  - TSS:

    `TSS LIST(acid)`

    `TSS LIST(ACIDS) ACIDPRFX(acid)`

Finding Dataset or Resource Access

- Listing a resource's accessors
  - RACF:

    `LISTDSD`

    `RLIST`

    `SEARCH`
  - ACF2:

    `ACCESS`
  - TSS:

    `TSS WHOOWNS`

    `TSS WHOHAS`

Mainframe Security Modes

- Modes
  - Initial Installation
  - Implementation
  - Locked-down
- RACF:
  - WARNING operand on the ADDSD, RDEFINE, ALTDSD, and RALTER commands
- ACF2:
  - MODE=(QUIET | LOG | WARN | ABORT | RULE)
- TSS:
  - MODE(DORM | WARN | IMPL | FAIL)

Admin Authority

- RACF:
  - SPECIAL, AUDITOR, OPERATIONS Attributes; scoped using group-versions
  - CLAUTH, Access and Profile Ownership
- ACF2:
  - ACCOUNT, SECURITY, LEADER, CONSULT, USER
  - Scoped by SCPLIST field defined in logonid record
- TSS:
  - ACID types: User, DCA, VCA, ZCA, LSCA, SCA
  - TSS AUTH ACID, RESOURCE, FACILITY, DATA, MISC1, MISC2, MISC3, MISC4, MISC5, MISC7, MISC8, MISC9, SCOPE
  - CASECAUT special resource class

Utilities: RACF

IRRMIN00	Format a RACF dataset, update RACF templates from release to release
IRRUT100	Cross reference utility (replaced by IRRDBU00 – Database Unload Utility)
IRRUT200	Verify database organization
IRRUT300	BLKUPD command for viewing/modifying (zapping) bits and bytes
IRRUT400	Split, merge, extend, reorganize database
IRRDBU00	Create column-oriented flat file suitable for browsing, REXXing, or loading into relational database
IRRIRA00	Create alternate index structure
RVARY command	Activate, deactivate, switch RACF databases

Utilities: ACF2 (Reporting)

ACFESAGE	ACF2 Database Offload to Flat File
ACFRPTDA	MLS DIRAUTH Event Log
ACFRPTCR	TSO Command Statistics Log
ACFRPTDS	Data Set/Program Event Log
ACFRPTEL	Infostorage Update Log
ACFRPTIX	Data Set Index Report
ACFRPTJL	Restricted Logonid Job Log
ACFRPTLL	Logonid Modification Log
ACFRPTNV	The Environment Report
ACFRPTOM	UNIX System Services (USS) Report
ACFRPTPP	The Preprocessor
ACFRPTPW	Invalid Password/Authority Log
ACFRPTRL	Rule-ID Modification Log
ACFRPTRV	Resource Event Log
ACFRPTRX	The Logonid Access Report
ACFRPTSG	CA Statistics Report - Cache, CPF, SAF, OMVS Stats
ACFRPTSL	Selected Logonid List
ACFRPTST	The SAF Trace Report
ACFRPTWS	The WorkStation Utility
ACFRPTXR	The Cross-Reference Report

Utilities: ACF2

ACFBATCH	Execute sequence of ACF subcommands in batch
ACFBCOMP	Compile rule sets in batch
ACFBDCMP	Decompile rule sets into z/OS data sets in batch
ACFBSYNC	Synchronize TSO BRODCAST with the CA ACF2 Logonid database in Batch
ACFCOMP	Compile/Decompile access rule sets - TSO Command
ACFESGP	Convert source group cross-reference records in Batch
ACFMERGE	Updates the logonid database with the most current password in Batch
ACFNRULE	Add or delete selected rules in Batch or TSO
ACFRGP	List resource name and associated group names in Batch
ACFRULCU	Deletes rules for a particular logonid or UID from the database in Batch
ACFXREF	Identifies INCLUDE or EXCLUDE values associated with cross-reference records
ACFDEL	File erasure in TSO
ACFERASE	File erasure in Batch
ACFSUB	Controlled submission of batch jobs in TSO
SAFCRRPT	Certificate Display Utility in Batch
ACFIDMAP	IDMAP Cleanup Utility in Batch
JOBCOPY	Controlled submission of batch jobs
LDSRPT	Lists all LDS requests stored in the LDS Recovery File

Utilities: TSS

TSSUTIL	Processes security-related activity that is recorded in SMF and the TSS Audit/Tracking File.
TSSTRACK	Allows administrators & auditors to monitor security-related events in real time
TSSAUDIT	Allows an auditor to monitor changes to the TSS security file and monitor other sensitive MVS data.
TSSCHART	Builds a tree structure of the full TSS Security File representing divisions, departments, profiles, and users.
TSSCPR	Batch utility that gives the user the ability to produce customized reports extracted from the CPF Recovery File.
TSSRPTST	Processes and displays the output that was sent to SMF by the SAF SECTRACE command.
TSSOERPT	Processes security-related activity recorded in SMF data sets to monitor user activity in Unix Systems Services(USS)
LDS Recovery	The LDS recovery report (LDSRPT), lists all LDS requests stored in the LDS Recovery File.
Cert utility	Utility to display the certificate hierarchy in your database.
TSSRPTSG	Report on CA Top Secret statistics such as Sysplex, Cache, CPF, CMDSTATS, Workload, IOSTATS, RACROUTES & SECCACHE
TSSCFILX	Query TSSCFILE data without creating additional security file overhead.
TSSCHKDN	Utility that identifies invalid distinguished names (DNs) for CA Top Secret IDMAP users
TSSSIM	Utility to test permissions on the Security File without affecting the production environment.
TSSFAR	File Analysis Routine (TSSFAR) to review the permissions and assignments recorded in the Security File.
TSSRECVR	Security file recovery is performed by applying the TSSRECVR routines to the backup security file.
TSSXVSDT	Batch utility that assists in backing out of the VSAM digital certificate feature.
SECTRACE	SECTRACE command to trace any security request made to the System Authorization Facility (SAF).
TSSCFILE	Batch utility that produces customized reports extracted from the CA Top Secret Security File.

Now this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning.

Sir Winston Churchill (1874 - 1965)

Where to Find Out More

- CA ACF2, CA Top Secret manuals and related content
  - Available on-line at https://techdocs.broadcom.com/
- IBM RACF Manuals and Redbooks
  - Available on-line at ibm.com

Questions? I'm Reg at Harbeck dot ca 🇨🇦