A Mainframe Security Rosetta Stone – Translating Between Mainframe Security Products

Reg Harbeck

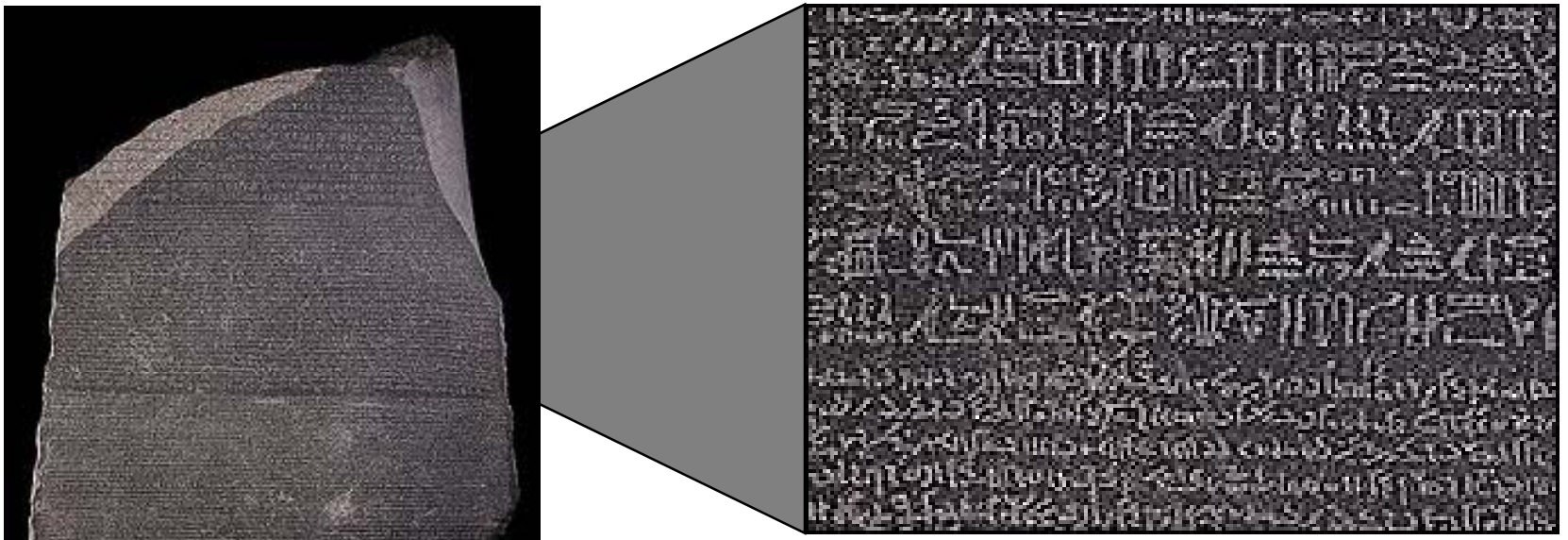
2009-08-24
Session #5461

Agenda

- What's a Rosetta Stone?
- About this session
- Introducing the z/OS security packages
  - RACF
  - ACF2
  - 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

- RACF
- CA 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

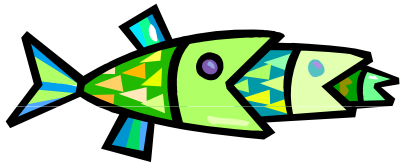
- Resource Access Control Facility
- The original mainframe security system (1976)
  - Unless you count UADS, the password file and dataset protection bits
- Uses dataset protection bits with discrete profiles; deleted with protected object
- Generic profiles more policy-based, not attached to objects secured
- IDs are called “user IDs”

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
  - One primary and one secondary (backup)

CA 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



- "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

CA 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

CA 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)

CA 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)
    - 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)

CA Top Secret

- “Top Secret” aka “TSS”

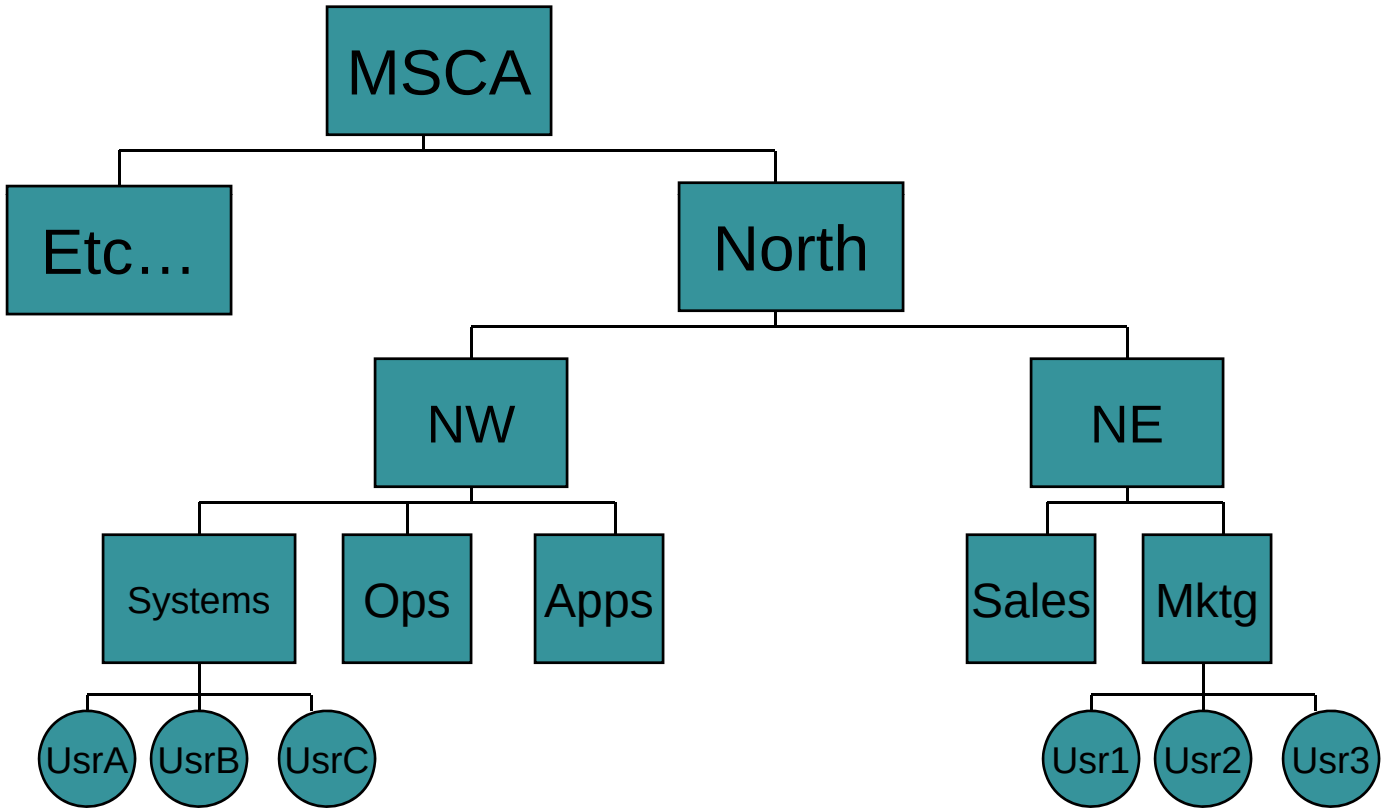
- Developed by CGA Software Products Group in 1981
- Acquired by CA in 1985

CA Top Secret

- Security database: one file
- IDs are called “ACIDs” (pronounced **ay**-sids, for ACcessor IDs)
- Tree Structured
  - Everything (including ID’s) 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”

CA Top Secret

- Hierarchical organization



Zone

Division

Department

Users

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:
    - 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:
    - 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
  - ACF2:
    - SET LID
    - CHANGE *logonid* CICS
  - TSS:
    - TSS ADDTO(*acid*) FACILITY(CICS)

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' *UACC(*access*)*
    - Generic profile:

      ADDSD 'dsname-incl-generic-char' *UACC(*access*)*
    - **or**

      ADDSD 'dsname' *UACC(*access*) GENERIC*
  - ACF2:

    $KEY(*high-level-qualifier*)

    dsname-extent UID(*pattern-for-UIDs*) R(A) *and/or other accesses*
  - TSS:

    TSS ADDTO(*acid*) DSNAME(*dsname*)

Access

- Permitting Access to Datasets
  - RACF:
    - PERMIT '*dsname-or-profile* ' ID(*userid*) ACCESS(*access*)
  - ACF2:

    $KEY(*high-level-qualifier*)

    dsname-extent UID(*pattern-for-UIDs*) R(A) *and/or other accesses*
  - TSS:

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

Access

- Grouping Access
  - RACF:

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

    SET LID

    CHANGE *logonid* DEPT(*dept*)
  - 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*)

Digital Certificates

- PKI / X.509
- Use public/private keys
- Enable more secure authentication, non-repudiation
- On z/OS you can use, administer and export keys

Digital Certificates

- To Add a Certificate
  - RACF:
    - RACDCERT ID(SYSMAN) ADD(MY.CERT) WITHLABEL('MIGRATED.KEY')
      PCICC(*)
  - ACF2:
    - Set profile(user) div(certdata)
    - INSERT SYSMAN.cert DSN('MY.CERT') LABEL(MIGRATED.KEY) TRUST PCICC PKDSLBL(*)
  - TSS:
    - TSS ADD(sysman) DIGICERT(EKMAUT01) HITRUST +
      DCDSN('MY.CERT") +
      LABLCERT('MIGRATED.KEY') PCICC +
      LABLPKDS('IRR.DIGTCERT.CERTAUTH.EKMAUT01')

Digital Certificates

- To Export a Certificate to z/OS dataset “MY.CERT”
  - RACF:
    - RACDCERT ID(SYSMAN) EXPORT(LABEL('SECURE.KEY')) DSN(MY.CERT)
      FORMAT(CERTDER)
  - ACF2:
    - Set profile(user) div(certdata)
    - EXPORT SYSMAN LABEL(SECURE.KEY) DSN(‘MY.CERT’) FORMAT(CERTDER)
  - TSS:
    - TSS EXPORT(sysman) DIGICERT(EKMAUT01) + DCDSN(‘MY.CERT') + FORMAT(CERTDER)

Displaying User Security Settings

- Listing a user's information
  - RACF:

    LISTUSER *userid*
  - ACF2:

    SET LID

    LIST *logonid*
  - TSS:

    TSS LIST(*acid*)

Mainframe Security Basics

- Modes
  - Initial Installation
  - Implementation
  - Locked-down
- RACF:
  - WARNING operand on the ADDSD, RDEFINE, ALTDSD, and RALTER commands
  - SETROPTS NOPROTECTALL | PROTECTALL specifies security for all datasets
    - PROTECTALL requires SETROPTS GENERIC(DATASET)
  - SETROPTS PROTECTALL(WARNING)
- 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

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 Cookbook, CA Top Secret Cookbook and related manuals
  - Available on-line at support.ca.com
- For more certificate information see support.ca.com documents TEC448158 for ACF2 and TEC436087 for Top Secret
- IBM RACF Manuals and Red Books
  - Available on-line at ibm.com

Questions / Discussion