A Mainframe Security Rosetta Stone

Translating Concepts and Commands Between Mainframe Security Products

Reg Harbeck
Mainframe Analytics Ltd.
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

- 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
• 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 or more pairs of primary and backup
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
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

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
ACF2

- Rules:
  
  $\text{KEY(SYS1)}$
  
  \text{BRODCAST UID(CHFSPSYS) R(A) W(A) A(L) E(A)}$
  
  \text{BRODCAST UID(*) R(A) W(A)}$
  
  \text{PARMLIB UID(CHFSPSYS) R(A) W(A) A(L) E(A)}$
  
  \text{PARMLIB UID(*)}$
  
  \text{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)
• 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)
Top Secret

- “Top Secret Security” aka “TSS”
- Developed by Northern Lights Software in 1981
- Acquired by CGA Software Products Group
- Acquired by CA in 1985
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”
Top Secret

- Hierarchical organization

MSCA
  - Etc...
  - North
    - NW
      - Systems
      - Ops
      - Apps
    - NE
      - Sales
      - Mktg

UserA, UserB, UserC

Zone
  - Division
  - Department
  - Users

Complete your session evaluations online at www.SHARE.org/Orlando-Eval
Defining IDs

• RACF:
  ADDUSER user_id DFLTGRP(group) PASSWORD(pwd) OWNER(group/user)

• ACF2:
  SET LID
  INSERT logonid PASSWORD(pwd) [some uidstring field(s)]

• TSS:
  TSS CREATE(acid) 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(PROC(logonproc))
  – ACF2:
    • SET LID
    • CHANGE logonid TSO
  – TSS:
    • TSS ADDTO(acid) FACILITY(TSO)
Controlling System Entry

• CICS
  – RACF:
    • ALTUSER userid CICS(OPCLASS(opclass))
      – Or just permit application id in class APPL
  – ACF2:
    • SET LID
    • CHANGE logonid CICS CICSCL(opclass)
  – TSS:
    • TSS ADDTO(acid) FACILITY(CICS) OPCLASS(opclass)
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-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 ADDDTO(acid) PROFILE(profilenname)
Passwords

• Changing a Password
  – RACF:
    ALTUSER userid PASSWORD(newpwd)
  – 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
  – ACF2:
    SET LID
    LIST logonid
  – TSS:
    TSS LIST(acid)
Mainframe Security Basics

• Modes
  – Initial Installation
  – Implementation
  – Locked-down

• RACF:
  – SETROPTS PROTECTALL (FAILURES | WARNING) | NOPROTECTALL (datasets only)

• 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

• IBM RACF Manuals and Red Books
  – Available on-line at ibm.com
Questions / Discussion

Complete your session evaluations online at www.SHARE.org/Orlando-Eval