RACF/VM: Protecting your z/VM system from vandals and other cyberspace miscreants

Session 9127

Alan Altmark
z/VM Development, IBM Endicott, NY

Disclaimers

This presentation introduces the mechanisms used by the z/VM operating system to maintain system security and integrity.

References to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe on any of the intellectual property rights of IBM may be used instead. The evaluation and verification of operation in conjunction with other products, except those expressly designed by IBM, are the responsibility of the user.

The following terms are registered trademarks or trademarks of IBM Corporation in the United States or other countries or both:

IBM z/VM zSeries RACF z/OS

Other company, product, and service names, which may be denoted by double asterisks (**), may be trademarks or service marks of others.

LINUX is a registered trademark of Linus Torvalds.

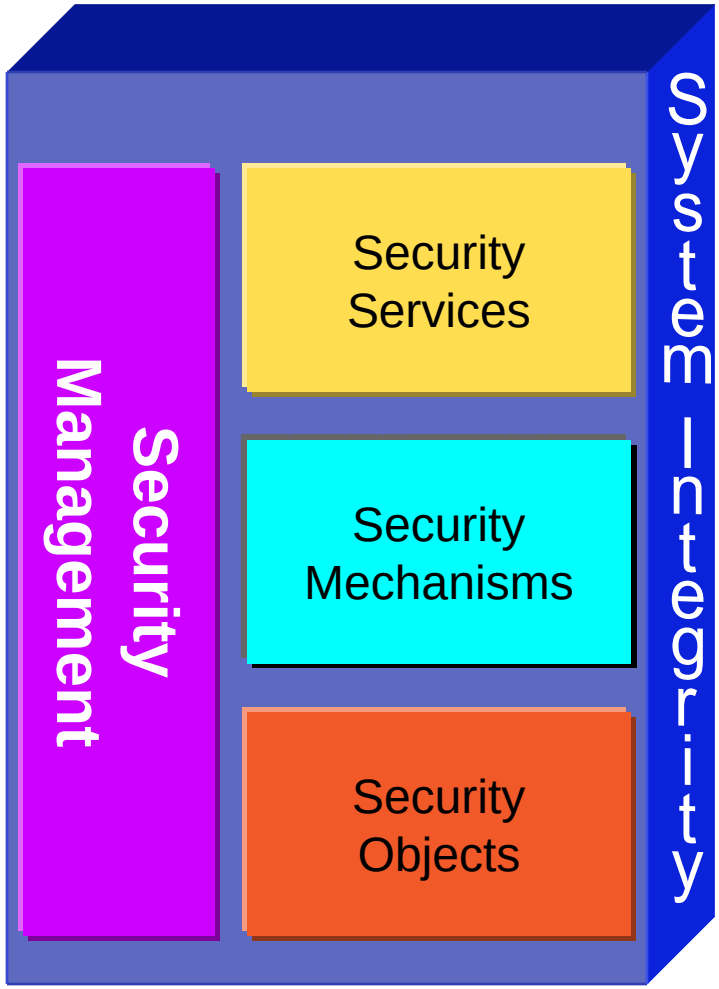
Agenda

- Security Architecture
- z/VM Security
- Augmenting Security with an ESM
- RACF support for z/VM
- References

Security Architecture

- System security
  - Identification & Authentication
    - –Identify users, ensure accountability
  - Access Control
    - –Limiting / controlling access to information
  - Auditing
    - –Verification of security policy enforcement
  - System Integrity
    - –Security mechanisms cannot be compromised
- Application security
  - RACROUTE for CMS applications

Based on ISO 7498-2



Immediate benefits of RACF

- Enhanced auditing, authentication, and access controls
- Encrypted user passwords
- Use Access Control List for minidisks instead of minidisk password
- Application integration
  - RACROUTE macro
  - CSL routines
- Feature of z/VM – already installed, CP kernel already built

Administration

- RACF Database
  - Profiles (entity records)
    - Users and groups of users
    - Protected resources
  - Global database options
  - Sharable among multiple systems
- Commands
  - Define users and groups
  - Control access to the system
  - Establish accountability
  - Delegate authority

Widgets

- Structure
  - db, backup db, audit 1, audit 2
  - CP modules
  - Administrator cmds
  - User cmds
- Management

User attributes

- Extraordinary system-wide privileges
  - SPECIAL - security administrator
  - AUDITOR - monitors system security
  - OPERATIONS - DASD maintenance
- Extraordinary user privileges
  - Group SPECIAL - local security administrator
  - Group AUDITOR - monitors security for the group
  - Group authorities - USE, CREATE, CONNECT, and JOIN

User Identification/Validation

- Password management
  - Only user knows the password
  - User can change his or her own password
  - Security administrator or hacker cannot read the password
    - 1-way DES encryption
  - Security administrator *can* reset the password (temporary)

User Identification/Validation

- Password policies
  - Required change interval
  - Expiration warnings
  - Rules for content and length
  - Re-use
  - Encryption (one-way DES is the default)
  - Exits are available to control generation and validation of passwords
- User policies
  - Automatic suspension of inactive users
  - Automatic revocation of users due to invalid password count
  - Notification of last system access

Authorization from a CP point of view

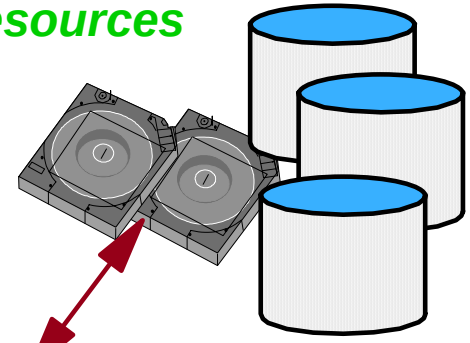
- Access rights are based on VM user ID or POSIX UID
- CP asks RACF “Does UserA have R/W access to UserB 191?”
- RACF responds:
  - Yes
  - No
  - Don’t know a.k.a “defer”

RACF for zVM

Users

User identification and authentication

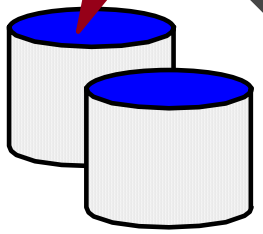
Resources



Security administration

RACF for z/VM

Resource authorization checking and system access control

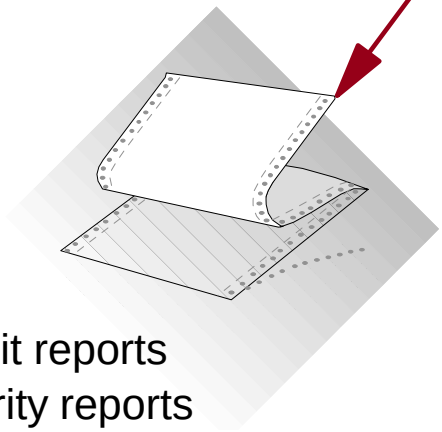


RACF database

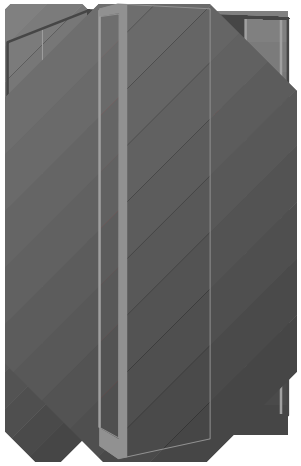
- Primary and backup
- Local (physical) sharing

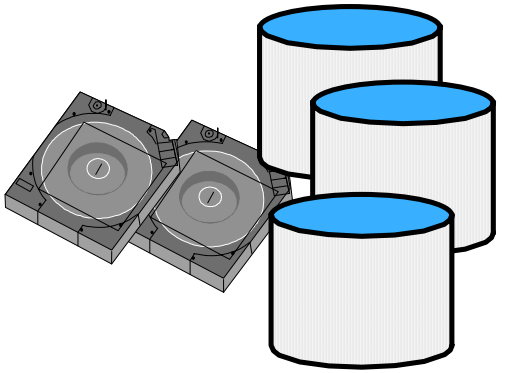
Security console

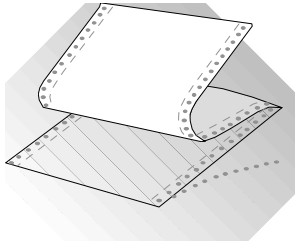
- Violation reporting

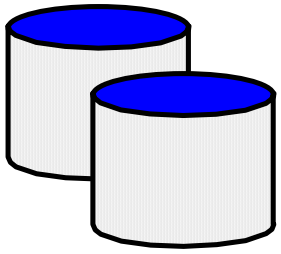


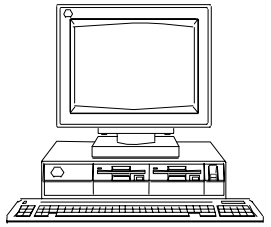
Audit reports integrity reports



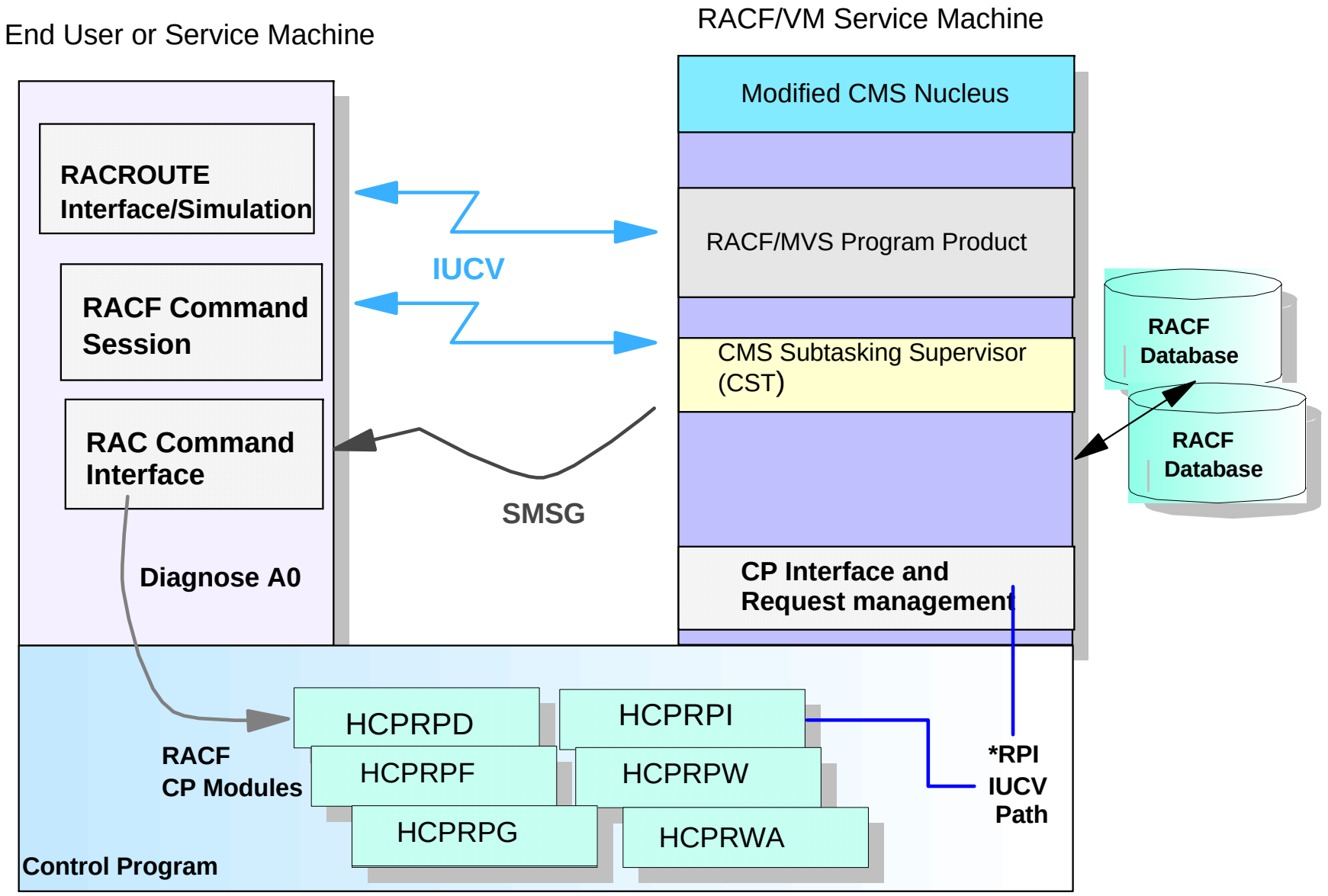




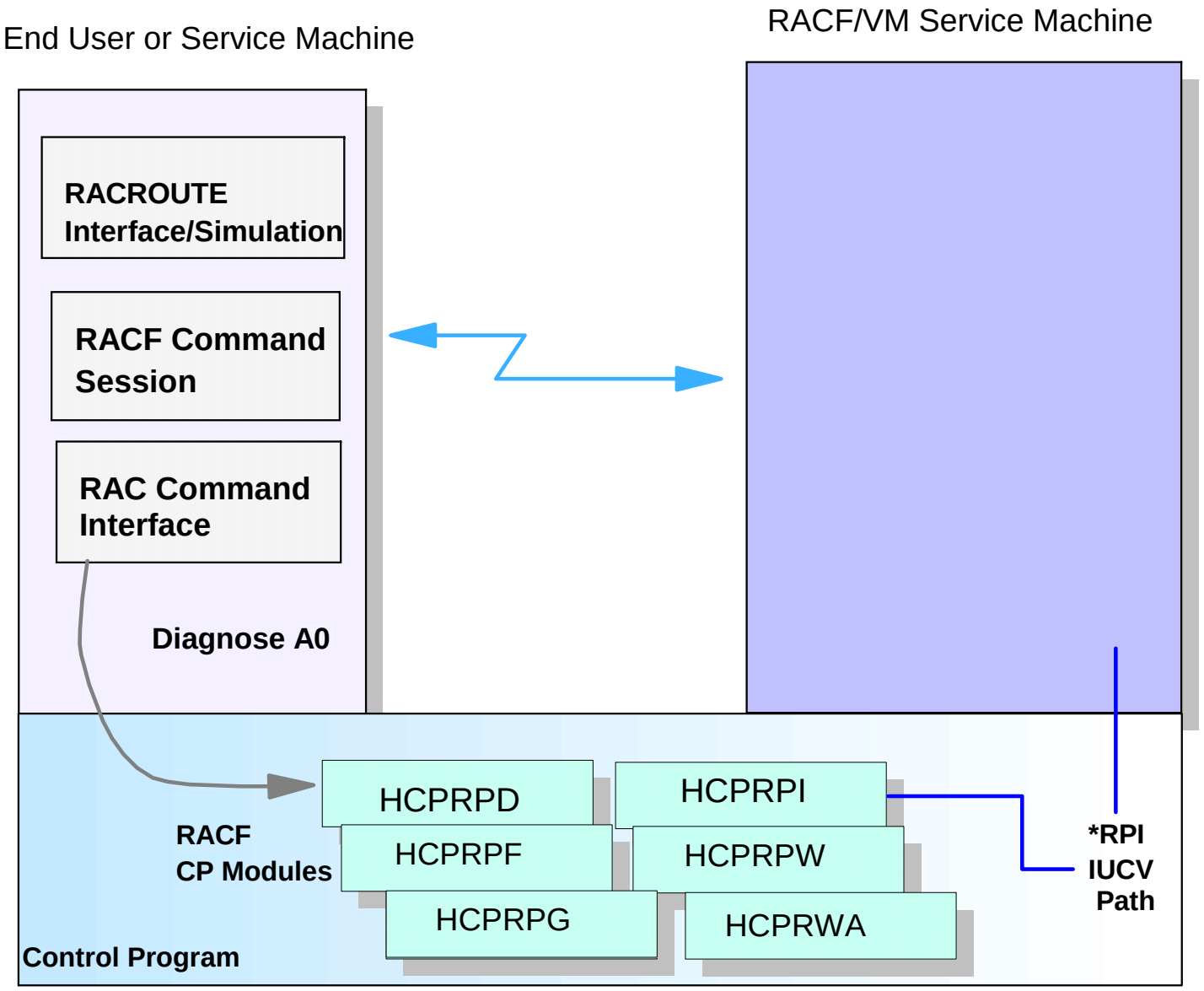




RACF for z/VM Structure

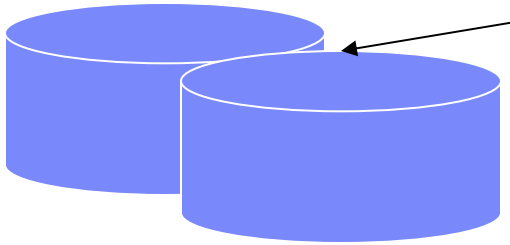


RACF for z/VM Structure



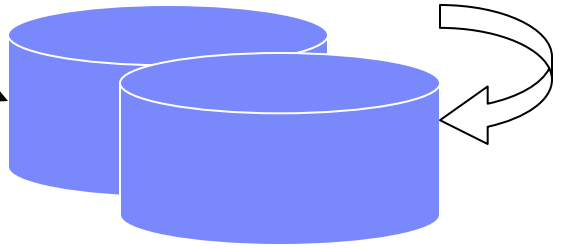
RACF Structure

Primary and backup database



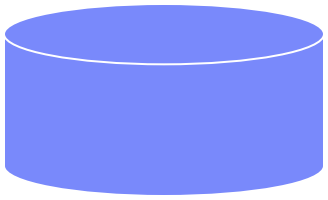
RACFVM

Alternating audit trails

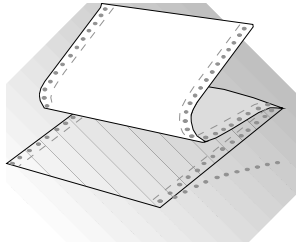


IBMUSER

Database load / unload



RACF Report Writer

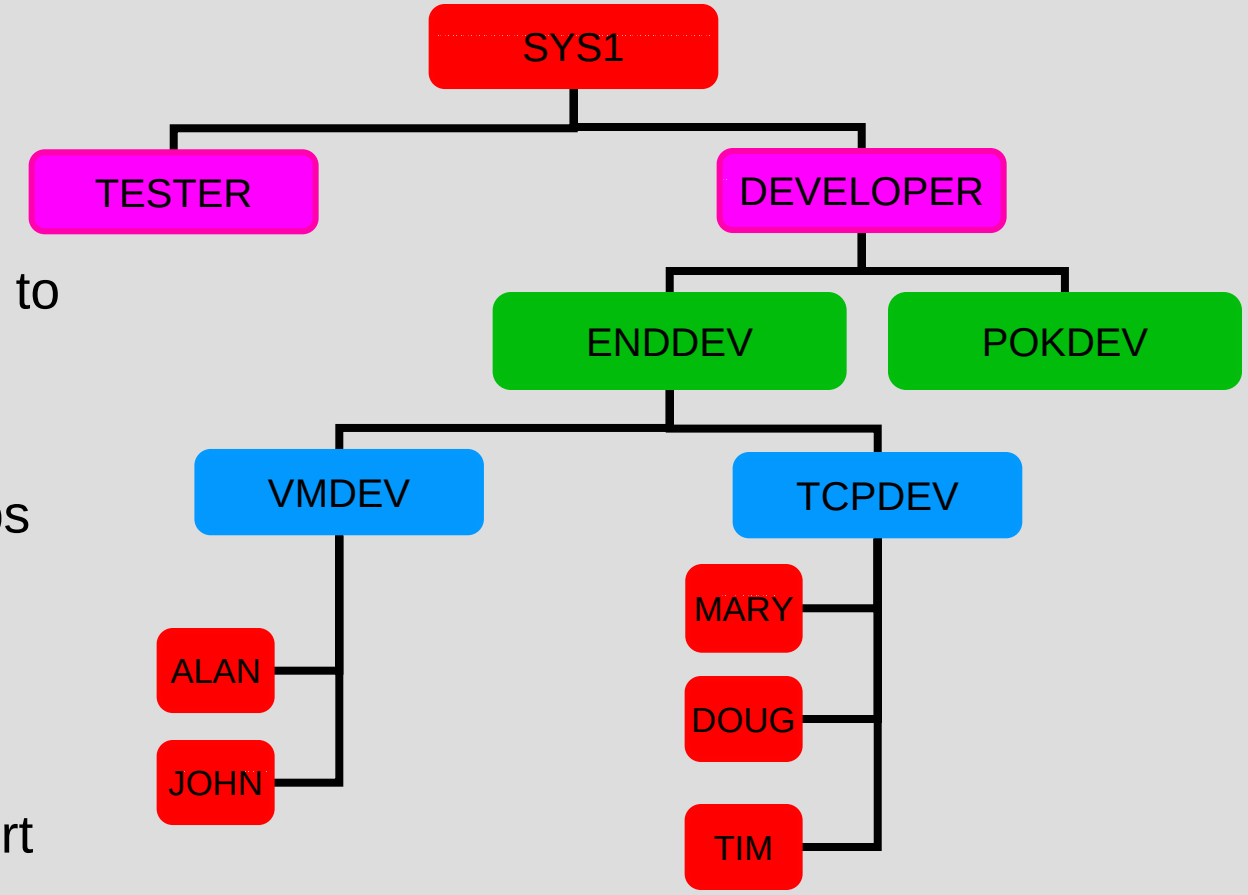


Features and Functions

- Protected system access
  - One-way DES password encryption
  - Where and when controls
  - Intrusion detection and defense
- Resource access control lists
- Groups
- Separation of duties: security admin, operations, auditor
- Multi-level security (MLS)
- Real-time violation notification
- Audit reporting tools
- Integrity verification tool (DSMON)
- Synergy with z/OS

RACF Group Structure

- Give access rights to a group
- Connect users to one or more groups
- Delegate group management
- Reduce administration effort



RACF Administrative Commands

FUNCTION	USER	GROUP	GENERAL RESOURCE
DEFINE	ADDUSER	ADDGROUP	RDEFINE
ALTER	ALTUSER	ALTGROUP	RALTER
LIST	LISTUSER	LISTGROUP	RLIST
DELETE	DELUSER	DELGROUP	RDELETE

Other RACF Commands:

- PASSWORD
  - Change password/interval
- PERMIT
  - Modify access list
- SEARCH
  - Locate RACF information
- CONNECT
  - Associate user with group
- REMOVE
  - Disassociate user from group
- SETROPTS
  - RACF installation security options
- SETEVENT
  - Convey to CP for which set of functions/commands CP is to invoke RACF
- SETRACF
  - Activate/Inactivate RACF
- RVARY
  - Turn RACF on/off

RACF Administrative Commands

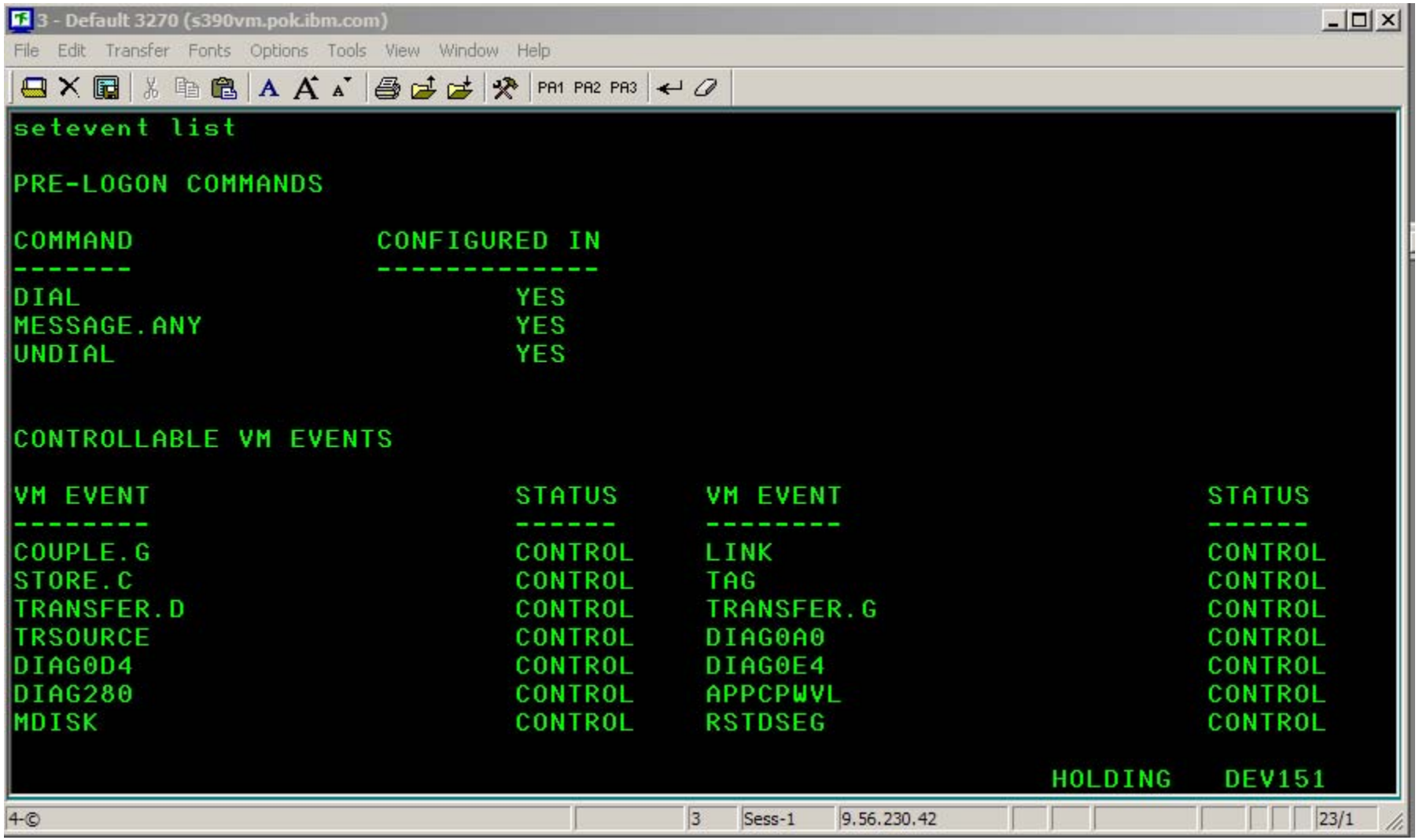
RACF control of z/VM Commands and Diagnoses

- Controlled by the SETEVENT command, and profiles in the VMXEVENT class
- The member list of a VMXEVENT profile specifies which CP functions are audited, and which are controlled
  - All CP command and diagnoses are auditable. None are audited by default
  - A subset of CP functions are controllable, as defined by z/VM. All are controlled by default. If a function is not controlled, authorization is determined by CP directory
- SETEVENT LIST shows which functions are being audited and controlled
- SETEVENT REFRESH is used to alter the settings in CP
- VMXEVENT profiles can be defined at an individual user level to override system-wide settings
- RPIDIRCT EXEC can prime RACF with definitions from CP directory

Control of z/VM Commands and Diagnoses…

- When a function is controlled using VMXEVENT, CP calls RACF to authorize a request when that function is used
- At this point, RACF protection is handled by:
  - Defining RACF profiles which provide the security definition of the protected resource
  - Activating the appropriate RACF class

SETEVENT Command output listing sample



RACF classes which control CP events

VMMDISK	Minidisk access via LINK command
VMRDR	Ability to send files to unit record devices of a user via TRANSFER, SPOOL, etc commands
VMNODE	Ability to send files to RSCS nodes using the TAG command
VMBATCH	Ability to work on behalf of another user using Diagnose 0xD4
VMSEGMT	Use of a restricted named saved segment (NSS) or discontinous saved segment (DCSS)
VMCMD	Various CP commands: STORE, XAUTOLOG, TRSOURCE, etc
VMLAN	Authorization to couple to a Guest LAN or Virtual Switch

RACF classes which control CP events

VMXEVENT	CP events that can be controlled or audited
VMMAC	Used with MLS support (SECLABELs)
VMPOSIX	OpenExtensions
SECLABEL	Information sensitivity and partitioning (MLS)
TERMINAL	Local, SNA, or telnet terminals
SFSCMD	Shared File System server operator commands
FACILITY	Use of RACROUTE macro
SURROGAT	LOGON BY
TAPEVOL	Tapes (if supported by tape management system)

Resource Profiles

- Profiles describe protection of resources
  - Maintained by security administrator and/or users
  - Per-defined or defined automatically
  - Identifies owner of profile
  - Logging information
  - Universal access authority
  - Access list
  - “warning” indicator
  - Security classification
  - Notification settings
  - Access statistics

```
RDEFINE VMLAN SYSTEM.LAN1 UACC(NONE)
PERMIT SYSTEM.LAN1 CLASS(VMLAN) ACCESS(READ) ID(BRUCE)
```

Access Rights

- Hierarchical
  - NONE
  - READ – read-only
  - UPDATE – read and write
  - CONTROL – read, write, plus control operations (if any)
  - ALTER – Full access, plus can change access list
- Precise access depends on resource class. For minidisks it controls the allowed LINK modes:
  - READ - R, RR, SR, ER
  - UPDATE - W, WR, SW, EW
  - CONTROL - M, MR, SM
  - ALTER – MW

Example – protecting a minidisk

- `RDEFINE VMMDISK BRUCE.191 UACC(NONE)`
- `PERMIT BRUCE.191 CLASS(VMMDISK) ID(ALAN) ACCESS(READ)`
- `RDEFINE VMMDISK MAINT.190 UACC(READ)`
- `SETROPTS CLASSACT(VMMDISK) RACLIST(VMMDISK)`
- `RALTER VMXEVENT MYEVENTS ADDMEM(LINK/CTL)`
- `SETEVENT REFRESH MYEVENTS`

Logon controls

- RACF is called whenever a user enters the system via LOGON, AUTOLOG, or XAUTOLOG
  - This is unconditional – cannot disable in the VMXEVENT profile
- Passwords are one-way encrypted in the RACF database
- Undefined users cannot logon
- Can control which terminals a user can log on to using the TERMINAL class
  - Telnet IP addresses can be mapped into terminal names
    - 9.12.248.3 = 090CF803

Support for shared user IDs (LOGON BY)

- Define **LOGONBY.*userid*** in SURROGAT class and permit surrogate users with READ access
- Users specify LOGON <shared> BY <surrogate>, specifying their own password
- Audit trail identifies shared and surrogate user IDs for subsequent authorizations
- Shared users cannot be logged onto directly by default.
  - Can be allowed by permitting user to its own SURROGAT class profile

Support for OpenExtensions (UNIX)

- OVM segment of USER profile contains
  - UNIX UID
  - Initial working directory
  - path name of shell program (similar to z/OS use of OMVS segment for Unix System Services)
- OVM segment of GROUP profile contains GID
- Protection and auditing of files and directories in the Byte File System
- Protection of ability to execute set-UID and set-GID files with profiles in the VMPOSIX class. Extends granularity to an individual's ability to switch effective identity to a specific UID or GID.
  - Execution of set-UID and set-GID files is prevented by default

Support for Shared File System (SFS)

- Protection and auditing of SFS files with profiles in the FILE class
  - ADDFILE, ALTFILE, etc commands provided to manipulate resources using SFS file syntax
  - Improve usability with the ability to use SFS file syntax (vs. RDEFINE, RALTER, etc)
- Protection and auditing of SFS directories with profiles in the DIRECTRY class
  - ADDDIR, ALTDIR, etc commands provided (similar to file commands)
- Protection and auditing of SFS operator and administrator commands with profiles in the SFSCMD class

Multiple RACF service machines

- Can configure several servers running concurrently to increase throughput of CP requests
- All servers share a common RACF database
- Individual servers can be dedicated to specific application servers
  - SFS, BFS
  - Or other application server
- Available only when using ECKD disk

RACF Monitoring

- Immediate notification of abnormal security events
  - Sent to system operator console
    - As defined in CSTCONS table
  - Optionally sent to resource owner
- Types of messages
  - Unsuccessful system accesses
  - Unsuccessful attempts to access resources
  - Failed RACF commands due to insufficient authority
- Messages include who caused the failure and what they were trying to do

RACF Journaling

- Logging of
  - Database status
  - Failed attempts to access the system
  - Resource access (optional)
    - Successes, failures, or both
      - READ, UPDATE, ALTER, CONTROL
  - Access granted with a warning
  - “Failsoft” decisions made by the system operator
- Options can be set by profile owners or auditors

RACF Journaling

- Auditor controls
  - Users
  - SPECIAL users
  - Resources
  - Resource classes
  - RACF command violations

Summary

- RACF for z/VM enhances security for z/VM by:
  - Providing fine-grained access controls of VM resources used by users and guests
    - Permits the sharing of VM UserIDs with accountability
  - Auditing capability of VM events – CP commands, diagnoses, access of resources, and authentication
  - Separates the disciplines of security Administrator, Auditor and operations staff
  - Passwords are encrypted, not stored in clear-text.
- Utilities which enable the examination of audit data and security database rules for reporting and data mining
- Depends upon the base system integrity provided by both the z/VM operating system and the zSeries

Resources and References

- RACF for VM publication library
  - Especially the Security Administrator's Guide
    http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/ICHVM07
- z/VM Security and Integrity
  http://www.ibm.com/servers/eserver/zseries/library/techpapers/gm130145.html
- Security Evaluations for IBM Products
  http://www.ibm.com/security/standards/st_evaluations.shtml
- IBM Security Solutions
  http://www.ibm.com/security
- IBM Global Services – Security and Privacy Services
  http://www.ibm.com/services/security/

Contact Information

- By e-mail: Alan_Altmark@us.ibm.com
- In person: USA 607.429.3323
- On the Web: http://ibm.com/vm/devpages/altmarka
- Mailing lists: IBMTCP-L@vm.marist.edu
  VMESA-L@listserv.uark.edu
  LINUX-390@vm.marist.edu

  http://ibm.com/vm/techinfo/listserv.html