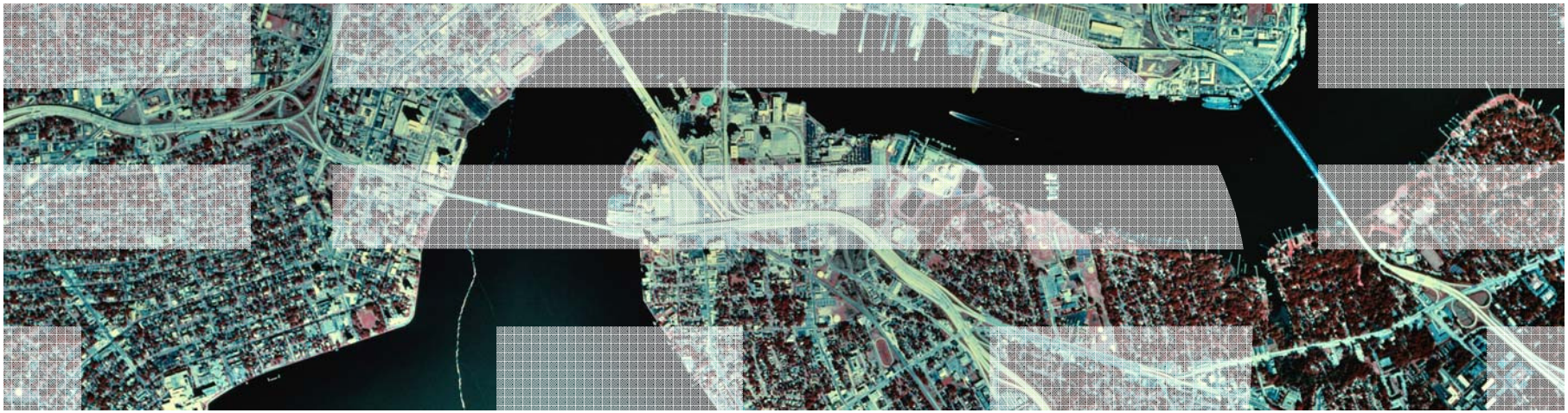
Brian W. Hugenbruch CISSP, z/VM Security Architect
bwhugen@us.ibm.com
SHARE – February 2011 - Anaheim

Securing z/VM: The Road to EAL 4

or “How to dig a moat, raise the drawbridge, lower the portcullis, and prepare the boiling oil”

Session 8439 -- written by Alan Altmark, IBM Lab Services



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

DB2	System z9
DS8000*	System z10
IBM*	z9*
IBM eServer	z10
IBM logo*	z/OS*
System z	z/VM

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Intel is a trademark of Intel Corporation in the United States, other countries, or both.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

Red Hat, the Red Hat "Shadow Man" logo, and all Red Hat-based trademarks and logos are trademarks or registered trademarks of Red Hat, Inc., in the United States and other countries.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

- Common Criteria definitions
- System Requirements
- CP configuration requirements
  - IPL
  - SYSTEM CONFIG
  - AUTOLOG1
- RACF requirements

This presentation is for illustration purposes only, and is not a complete description of all steps required to place your system into the evaluated configuration.

Your configurations may be *more* stringent than those used in Common Criteria.

For a complete description, consult the z/VM Secure Configuration Guide.

Common Criteria

- An international standard, ISO 15408
- Security Target: The Claim
  - Protection Profiles
    - Standard
    - CAPP, LSPP, OSPP, SKPP, MLOSPP, …
  - Enumerated function
- Evaluation Assurance Level (EAL)
  - The proof, on a scale of 1 to 7
    - 1 = “Because they say so”
    - 2-6 = everthing in between 1 and 7
    - 7 = Mathematical proof with exhaustive tests

Certification

- z/VM V5.1 EAL 3+ CAPP/LSPP
- z/VM V5.3 EAL 4+ CAPP/LSPP
- z/VM V6.1 EAL 4+ OSPP with labeled security extensions
  - **Evaluation in progress**

Basic system assumptions

- You have the RACF Security Server feature enabled
- The Common Criteria evaluation was done with RACF
- No evaluation was done for any other ESM and so no claim can be made about the security characteristics of those other ESMs

Discretionary access control

- The mechanisms that are provided for resource owners (end users) to manage the access list of resources they own
  - RACF PERMIT
- These override many of the CP directory privileges

Mandatory access control

- Controls that are established by the security administrator that **override** discretionary controls
  - They turn “allowed” into “denied”
  - Never “denied” into “allowed”
- Every user and resource has a security *label*

Security Label Math

- The label contains information on
  - The *sensitivity* of the information
    - Secret, Top Secret, Secret Squirrel, “For Your Eyes Only”
  - The *type (category)* of information
    - QUANTUM, AREA52, MORTGAGE, HEALTH

- Labels can contain more than one category, but the access rights math gets more difficult
  - Resources labels should contain exactly one category
  - User labels should contain all of the categories the user has access to

Security Label Math

- Read-only: The resource's assigned category must be in the user's label
- Write-only: All of the user's assigned categories must be in the resource's label
  - There are no resources with W/O access
  - Only applies to user-to-user (CP MSG)
- Read-write: The user's and the resource's assigned categories must be identical

System Startup

- No one is allowed to access the system or its resources until the ESM is up except the system IDs identified in SYSTEM CONFIG:
  - AUTOLOG1
  - OPERATOR
  - OPERACCT (DISKACNT)
  - OPEREREP (EREP)
  - OPERATNS
  - OPERSYMP
- Their authorizations are from CP
- Let ESM post-initialization processing bring up workload
  - AUTOLOG2

System Startup

- DRAIN DISABLE at IPL prompt
  - Needed only for channel-attached printers
- AUTOLOG1 must not do anything that allows workload to start or users to access the system until the ESM is up
  - VARY ONLINE and ATTACH to SYSTEM is ok
  - Only XAUTOLOG RACFVM
  - XAUTOLOG ESM ok
  - No ENABLE or START

SYSTEM CONFIG

- These FEATURES must be configured with DRAIN NOENABLE
  - AUTO_IPL
  - AUTO_IPL_AFTER_RESTART
  - AUTO_IPL_AFTER_SHUTDOWN_REIPL
- If the operator's console is not physically secure
  - Operator must authenticate
  - SYSTEM_USERIDS OPERATOR *operator* DISCONNECT

SYSTEM CONFIG

- No passwords on command lines
  - `FEATURES PASSWORDS_ON_CMDS AUTOLOG NO LINK NO LOGON NO`
- Erase residual data on T-disks
  - `FEATURES ENABLE CLEAR_TDISK`
- If you have dedicated disks or full-pack minidisks, prevent duplicate volid problems
  - `DEVICES OFFLINE_AT_IPL 0000-FFFF`
    `DEVICES ONLINE_AT_IPL rdev1 rdev2 rdev3-rdev8`
  - Then bring remaining devices online in AUTOLOG1 and ATTACH to SYSTEM as required

CPLOAD module

- Must be configure to FAIL any resource access request that RACF defers (for those classes that will be active)

- RACF HCPRWA options
  - HCPRWAC is a special version of HCPRWA that is pre-configured to fail requests

Directory

- Anonymous access not allowed – no NOPASS users

- Untrusted virtual machines may not
  - Be the target of another virtual machine's CONSOLE statement
  - Have IUCV with the ANY or *IDENT RESANY operand
  - Have OPTION with any of the following operands:
    - COMSRV
    - DEVMaint
    - DIAG88
    - DIAG98
    - D84NOPAS
    - MAINTCCW

Directory

- No minidisk overlaps except for those used for backups or where explicitly required

TCP/IP

- SYSTEM DTCPARMS and server configuration files may not enable anonymous access.
- Only the telnet server and stack were evaluated.
- No claims made about other TCP/IP functions (e.g. ftp)
  - Use common sense

RACF Security Server

- All users must be defined in RACF
  - If using labels, all users must have a default security label
- All resources in any activated class must be defined to RACF
  - Any resource not defined to RACF cannot be accessed

Required classes

- FACILITY – Enable RACROUTE processing
- VMXEVENT – Enable CP command and diagnose access controls
- VMCMD – Enable protection for certain CP commands and diagnose instructions
- VMSEGMT – Enable protection of shared memory objects (DCSS, NSS)
- VMRDR – Enable protection of spool file access
- VMBATCH – Enable protection of Diagnose 0xD4 (set alternate user ID)
- VMLAN – Enable protection of Guest LANs and virtual switches
- VMMDISK – Enable protection of minidisks

RACF Processing Options

- No DIAL or MESSAGE allowed before login
  - RAC SETEVENT NODIAL NOPRELOGMSG

- Passwords
  - Must be at least six characters long
  - Contain at least one numeric
    - Which may not be in the first or last position
  - User must be revoked if 5 invalid passwords are entered in a row
  - `SETROPTS PASSWORD(REVOKE(5)`
    `RULE1(LENGTH(6:8) ALPHA(1,6) ALPHANUM(2:5))`
    `RULE2(LENGTH(7) ALPHA(1,7) ALPHANUM(2:6))`
    `RULE3(LENGTH(8) ALPHA(1,8) ALPHANUM(2:7)))`

Password phrases

- Minimum of 14 characters long, so no requirement on construction except the rule that requires “non-trivial”.
  - Default RACF password phrase exit (ICHPWX11) already handles this

Your security policy

- You must have a security policy that deals with password expiration and your RACF configuration must enforce it.

- Password change frequency
  - 30 days? 90 days? A year?
  - Is it different for privileged users?

- Password reuse
  - How many passwords change intervals must pass before you can reuse passwords?
    - Watch for repeated uses of the PASSWORD or PHRASE command

RACF Processing Options

- Protect the STORE HOST command
  - Define a profile named STORE.C in the VMCMD class
  - Turn on auditing for STORE.C
  - Permit access to specific class C users
  - Only they can issue STORE HOST
- If RACF cannot record an event, the access must be denied and RACF must stop
  - SMF CONTROL file must say SEVER
  - Solution: Process SMF records daily

Special case for minidisks

- If more than one user needs R/W access to the same minidisk, use a generic VMMDISK profile: ALAN.0191*
- Grant ALTER access to the profile
- Disables the ability to alter the access list of the profile

Operations

- In order to ensure no residual data is present, you must format DASD before it is placed into service in a z/VM system.
- Protect dumps from unauthorized disclosure
  - They may contain sensitive data such as z/VM user IDs and passwords
- To change security labels, must ensure that they are not in use and that you have entered SETROPTS MLQUIET

Labeled Security

- Assign a label to every user
- Assign a label to every protected object
- Additional active classes
  - SECLABEL
  - VMMAC
- If you have CP-managed printers, extra configuration is required
  - See book
- Label SYSNONE exempts user of resource of label checking

Labeled Security

- Additional RACF configuration options (SETROPTS)
  - SECLABELCONTROL to prevent non-SPECIAL users from changing the contents of security labels
  - MLACTIVE(FAILURES) requires all users and protected objects to have a security label.
  - MLS(FAILURES) prevents declassification of data.
  - MLSTABLE prevents changes to security labels while they are in use and while the system is allowing users to login

Who runs in the evaluated configuration?

- No one
- It requires specific level of software and service level
  - It is invalidated by any other level
- It is the idea that you **can** place the system into an evaluated configuration and reproduce the environment that made the evaluators happy

Where to get more information?

- z/VM Secure Configuration Guide
  - Will place your system into the evaluated configuration
- Redbook: z/VM Security, SG24-7471

Dank u
Dutch

Merci
French

Спасибо
Russian

Gracias
Spanish

شكراً
Arabic

감사합니다
Korean

Tack så mycket
Swedish

धन्यवाद
Hindi

תודה רבה
Hebrew

Obrigado
Brazilian Portuguese

谢谢
Chinese

Dankon
Esperanto

Thank You

ありがとうございます
Japanese

Trugarez
Breton

Tak
Danish

Danke
German

Grazie
Italian

நன்றி
Tamil

děkuji
Czech

ขอบคุณ
Thai

go raibh maith agat
Gaelic