#SHAREorg

SHARE

z/VM Security Essentials

Alan Altmark
IBM Senior Managing z/VM Consultant

March 2014

SHARE in Anaheim

Notes

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 information contained in this document is for illustrative purposes only. It is not intended to define a complete security policy and implementation.

Topics

- Basic Assumptions
- Roles
- Authentication
- Authorization
- Security-sensitive commands and interfaces
- Audit
- Protecting the integrity of the CP kernel
- Centralized security management

Basic Assumptions

- The z/VM® system must generally conform to company and applicable regulatory policies
  - Evidence: SYSTEM CONFIG, USER DIRECT, audit trail
- A set of roles will be established
  - All virtual machines will have an assigned role
- An external security manager (ESM) will be used
- Every person accessing the system has their own user ID

Basic Assumptions

- System Programmers have the ability and the system-level authority to disable or bypass security controls
- System Programmers can access any data in the system
- System Programmers are trustworthy
  - Will obey security policy
- Violation of security policy has consequences to individuals

Roles

- Every virtual machine has a role to play
  - Security administrator
  - System programmer
  - System operations
  - Network administrator
  - Storage administrator
  - Service Virtual Machine
  - Workload (non-adminstrative)
    - Linux, CMS, z/OS®, etc.

Roles

- If it has no purpose, it does not belong.
  - NOLOG it.

- Administrators, system programmers, operations staff, and SVMs are trusted
  - All others (workload) are untrusted

Roles: Delegation and Separation

- Some people have multiple roles
  - Their user ID is authorized to perform all needed tasks
- Authority often delegated
  - E.g. DIRMAINT can be configured and authorized to issue privileged RACF® command (the Connector)
  - Separation of Duties may limit delegation
- Separation Of Duties
  - Security administration and system programming are handled by different people
  - Configuration does not implicitly create authorization
  - Driven by policy
  - Strict separation prohibits fully automated provisioning

Role: Security Administrator

- Assign each new virtual machine its proper role
- Establish and maintain effective password controls
- Establish and maintain security alerting procedures
- Ensure audit data is collected and archived as required by corporate policy
- Establish internal audit schedule
- Delegate any ESM rule definition to system programmers, as required
- Manage and monitor the ESM database
- Remain educated

Role: Security Administrator

- Privilege class G
- No provisioning authority
- Read access to ESM database
- No global data access rights
- Allowed to LOGON BY to ESM server(s)
- Shall have console monitored and recorded
- Can FORCE any user
- Shall have use of LINK command monitored

Role: System Programmer

- Responsible for the general well-being of the z/VM system
  - Provisioning of real and virtual resources
  - Monitoring and alerting
  - Performance
  - Disaster recovery and high availability
  - Automation
  - Security and integrity enablement
  - …
- May delegate some aspects to self-service applications
- Has complete access to all data

Role: System Programmer

- Privilege class: All
- Can add/delete/change resources in the ESM
- Full global data access rights
- Allowed to LOGON BY to any virtual machine except those designated as personal
- Shall have console monitored and recorded
- Shall have use of LINK command monitored

Authentication

- Access to system requires user ID and password or password phrase
  - Password is 1-8 characters, upper case, no special characters
  - Phrase is 9 or more characters, mixed case, any character
  - Longer passwords mean fewer rules are needed
- Only people have passwords or phrases
  - Exceptions for automated processes
  - Use XAUTOLOG or LOGON BY for others

Authentication

- Password and phrases must be
  - Non-trivial
  - Changed on a regular basis
    - The more powerful the user, the more often the password is changed.
  - Changed immediately after reset or new deployment
  - Encrypted
    - At rest: ESM encryption
    - In flight: z/VM SSL

Authentication: Fallback

- When ESM is down, only a small subset of users are allowed to login
  - Enables repair of the ESM
- For them, the password in the CP directory (USER DIRECT) is used

- Rules vary by ESM. RACF allows
  - Primary system operator (OPERATOR)
  - The RACF servers (RACFVM, RACMAINT)
  - The users identified by ALTERNATE_SYSTEM_OPERATORS in SYSTEM CONFIG

Authentication: Fallback

- Restrict access to USER DIRECT, as it contains sensitive data, even when an ESM is installed

Authorization

- Which CP commands or functions can a virtual machine use?
  - Privilege class
  - OPTIONS in the user directory
  - Those that can be controlled by the ESM
    - COUPLE, FOR, LINK, MDISK, STORE HOST, TAG, TRANSFER, TRSOURCE
    - Diagnose 0x88, 0xA0, 0xD4, 0xE4, 0x280, 0x290
    - Restricted DCSS/NSS

Authorization: Escalation of Privilege

- Escalation of privilege: Performing functions that your user ID is not duly authorized to perform
  - SET PRIVCLASS
  - Service Virtual Machines (SVMs)

Escalation of Privilege: SET PRIVCLASS

- Used to add or delete privileges
  - Only class C user can add privileges that are not in the target user's directory entry
- Very useful to confirm intent
  - Change SHUTDOWN to class S
  - COMMAND SET PRIVCLASS * -S in OPERATOR's directory entry
    - Requires SET PRIVCLASS * +S before issuing SHUTDOWN
    - Not accidental

Escalation of Privilege: SET PRIVCLASS

- Do not use this command to escalate a user's privilege unless there is an accompanying update to USER DIRECT
  - Only if needed to avoid painful logoff/logon (e.g. lost T-disk)

Escalation of Privilege: Service Virtual Machines

- Service Virtual Machines (SVMs) run programs that are used to help manage the activities of the system
  - RACFVM
  - DIRMAINT
  - TCPIP
  - PERFSVM
  - FTPSERVE
  - …
- They are privileged, so they should only run code from a trusted source

Escalation of Privilege: Service Virtual Machines

- Some SVMs accept arbitrary CP or other sensitive commands from an SVM-authorized user
  - NETSTAT CP, SMSG RSCS CP, DIRM CP, SSLADMIN SYSTEM
  - DIRM CMS RAC SETROPTS or PERMIT (!!)
  - Automation tools
- Accountability may be lost or blurred
  - Requires SVM audit log
- May be able to use exits to control

Escalation of Privilege: Service Virtual Machines

- Do not artificially force administrators to use SVMs
  - Not any safer than giving them the privilege they need
  - Promotes privilege escalation for convenience
  - "Attractive nuisance"

- However….

Escalation of Privilege: Service Virtual Machines

- Every rule has an exception (except this one?)
  - Escalation of privilege is allowed with management permission
    - If time is of the essence and permission cannot be reasonably obtained, management must be notified afterwards.
  - After the crisis is past, privileges are returned to normal
  - Repeated escalation indicates a problem with privilege assignments

Authorization: Access Rights

- Virtual machines with the same role need access to the same resources

- To simplify, use a group structure.
  - Authorize group
  - Add users to the group

Security-Sensitive Commands and Interfaces

- STORE HOST – Class C
  - Alters CP memory, data or code
  - Turn off the fences
  - Only use it when directed by Support Center
- SET SYSOPER – Class A
  - Can by used to effectively bypass OPERATOR confirmation or to hide notifications

Security-Sensitive Commands and Interfaces

- SET SECUSER – Class A, C, G
  - Take the virtual console from a user (A, C)
  - Give the virtual console to another user (G)
  - Issue commands and see output
- SET OBSERVER – Class A, C, G
  - See output of another virtual machine
  - Works while other virtual machine logged on, too

Security-Sensitive Commands and Interfaces

- SEND – Class C, G
  - Send command or replies to virtual machine console
  - Guest or CP
  - Class G requires SECUSER
  - Class C can send to any disconnected user
- XAUTOLOG … ON …. – Class A, B
  - Place virtual console on OSA-ICC or TN3270 session
  - Can give access to virtual machines you do not have LOGON BY or SECUSER access to

Security-Sensitive Commands and Interfaces

- FOR – Class C, G
  - Synchronously issue CP commands on another user ID
  - Class G requires LOGON BY or SECUSER
  - Class C can issue to anyone

Security-Sensitive Commands and Interfaces

- DEFINE MDISK – Class A
  - Must also be current system operator (SYSOPER)
    or
  - Must have OPTION DEVMAINT in the directory
  - Creates minidisk on any volume attached to SYSTEM
  - No ESM controls, so can DEFINE MDISK to create a minidisk overlay on a disk the issuer is not permitted to LINK

- Diagnose 0x04 – Class C, E
  - Programming equivalent of DISPLAY HOST
  - Treat them the same from an auditing perspective

Security-Sensitive Commands and Interfaces

- Diagnose 0x84 – Class B
  - Updates the active user directory without running DIRECTXA
  - OPTION D84NOPAS allows issuer to avoid the need to have the target user's password.
  - Only give to directory manager.

- Diagnose 0x88 – Class G (ESM control)
  - Validate passwords, verify LOGON BY authority, LINK to minidisks
  - If ESM defers, OPTION DIAG88 required.

Security-Sensitive Commands and Interfaces

- Diagnose 0xA0 – Class G (ESM control)
  - Perform privileged ESM-specific functions

- Diagnose 0xD4 – Class B (ESM control)
  - Allows issuer to change its identity for purpose of linking to minidisks, making IUCV or APPC connections, or creating spool files

Security-Sensitive Commands and Interfaces

- Diagnose 0xE4 – Class ANY (ESM control)
  - Obtain information about minidisks
  - Limited to own minidisks unless issuer has OPTION DEVMAINT or OPTION DEVINFO in the directory
  - With OPTION DEVMAINT, can also create fullpack minidisk overlays (similar to DEFINE MDISK)

Security-Sensitive Commands and Interfaces

- Diagnose 0x2C4 – Class B or OPTION LXAPP
  - Used to transfer data to/from Support Element
  - Used by FTP server
  - Can be used to transfer data outside of traffic monitors

- All of the preceding commands and functions need to be audited to ensure that they are not being misused

System Events

- Events recorded by ESM that indicate "something happened"

- DIRECTRY_CMD event
  - Generated when COMMAND statement is processed during LOGON
  - Issue any command, even those guest cannot itself issue

- SNIFFER_MODE event
  - Tells you when a guest that has promiscuous authorization on a VSWITCH enters/exits sniffer mode

Audit

- The audit trail is how you demonstrate conformance to the security policy

- You must define
  - Access restrictions
  - How often it will be collected
  - How often it will be reviewed
  - Where it will be archived and for how long

Audit

- With RACF, these are SMF records that can be sent to z/OS for processing or processed directly on z/VM
  - RACF Report Writer
  - zSecure for RACF
  - Vanguard
- Other ESMs have their own procedures

Audit

- If audit record cannot be written, then authorization must be denied
- "If there is no record of it, then it NEVER HAPPENED!"
- For RACF, specify SEVER YES in the SMF CONTROL file

Protecting the integrity of the CP kernel

- In addition to commands like STORE HOST, the CP kernel can be affected by other configuration items
- CPXLOAD
  - Loads code or data into the CP kernel
- CP_ADDON_INITIALIZE_ROUTINES
  - Run code in the CP kernel at IPL

Protecting the integrity of the CP kernel

- DEFINE COMMAND and ASSOCIATE EXIT
  - Add new commands or exits to the system
- MODIFY COMMAND, MODIFY DIAGNOSE
  - Alter the privilege class of commands and diagnose instructions

Protecting the integrity of the CP kernel Duplicate Volume Labels

- When there are duplicate volumes with the same label, CP chooses the volume with the lowest device number with the matching label (default behavior)

- Traditionally controlled using
  OFFLINE_AT_IPL 0000-FFFF
  ONLINE_AT_IPL …
  and subsequently ATTACH others to SYSTEM in AUTOLOG1

- In z/VM 6.3, use the RDEV option on CP_OWNED statement
  CP_OWNED SLOT 1 630RES RDEV 11F0

Protecting the integrity of the CP kernel

- QUERY IPLPARMS to find out what IPL parameters were used
- QUERY CPLOAD to find
  - The name and location of the CP load module
  - Location of PARM disk
  - Reason for system start
    - IPL
    - SHUTDOWN REIPL
    - System error
- QUERY CPLEVEL
  - Level of CP running
  - When system was IPLed
  - When CP load module was created

Centralized Access Controls – It's not just for CP!

- Applications (SVMs) can access ESM by using the RACROUTE macro
  - It is part of the formal z/VM interface specification
  - CSL routine available from IBM Lab Services
- Each SVM must be configured separately
  - DIRMAINT
  - Operations Manager
  - Backup and Restore Manager
  - Tape Manager
  - DFSMS
- Can eliminate separate authorization and audit files

Summary

- Your z/VM system needs to be bound by a cogent security policy
  - Roles
  - Authentication
  - Authorization
  - Accountability
  - Audit
- What is the point of securing the guests if you don't have demonstrable security of the hypervisor?
  - Doesn't matter whether you have one sysprog or a dozen

Contact Information

Alan C. Altmark

Senior Managing IT Consultant

IBM Systems Lab Services and Training

z/VM & Linux on System z

IBM

1701 North Street

Endicott, NY 13760

Mobile 607 321 7556

Fax 607 429 3323

Email: alan_altmark@us.ibm.com

Mailing lists:

IBMTCP-L@vm.marist.edu
IBMVM@listserv.uark.edu
LINUX-390@vm.marist.edu
http://ibm.com/vm/techinfo/listserv.html