



z/VM Security and Integrity

Alan Altmark
Security Strategist
z/VM Development
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

IBM logo

z/VM

RACF

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

© Copyright International Business Machines Corporation, 2002, 2008

Virtualization security risks being overlooked, Gartner warns

Gartner raises warning on virtualization and security.

Companies in a rush to deploy virtualization technologies for server consolidation efforts could wind up overlooking many security issues and exposing themselves to risks, warns research firm Gartner.

“Virtualization, as with any emerging technology, will be the target of new security threats,” said Neil MacDonald, a vice president at Gartner, in a published statement.

Network World
April 6, 2007

Agenda

- z/VM System Integrity
- z/VM Security
- IBM Commitment
- Customer responsibilities

Integrity

What is z/VM system integrity?

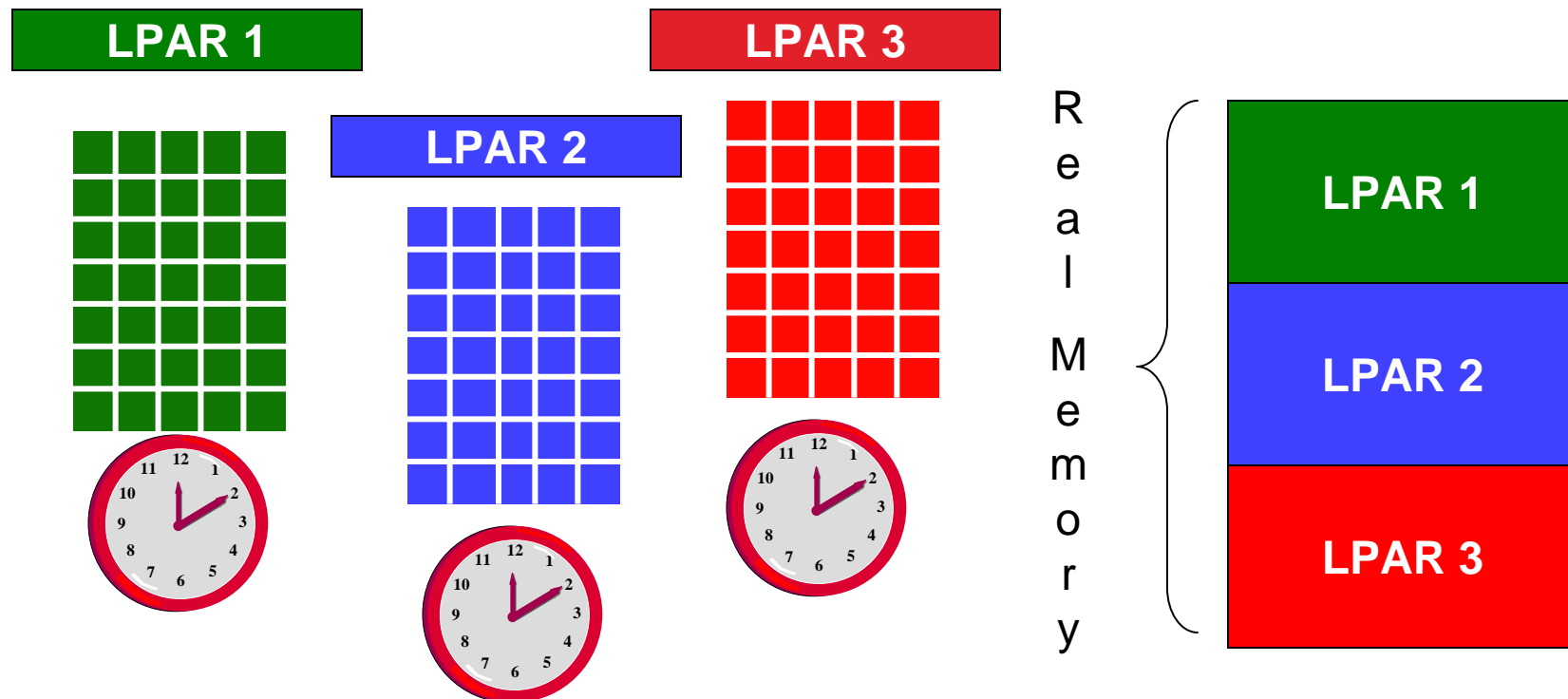
- The ability of the Control Program (CP) to operate without interference or harm, intentional or not, from the guest virtual machines
- The inability of a virtual machine to circumvent system security features and access controls
- The ability of CP to protect virtual machines from each other

Interpretive Execution Facility

- Start Interpretive Execution (SIE) instruction describes a virtual machine
 - ▶ Registers, PSWs, memory
 - ▶ Interception conditions (a.k.a. "SIE break")
 - Time slice expires
 - Unassisted I/O
 - Instructions that require CP's help
 - e.g. Set Clock
 - ▶ Certain program interrupts
- SIE runs until interception condition raised
- Basis for LPAR and virtual machines

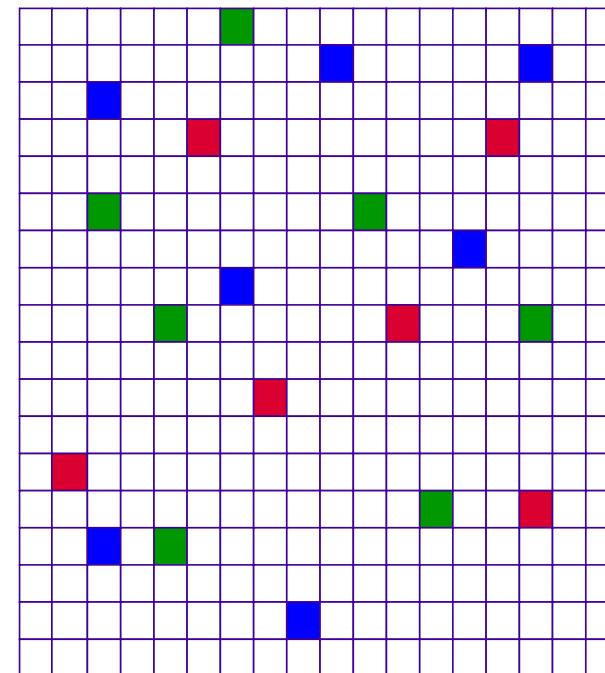
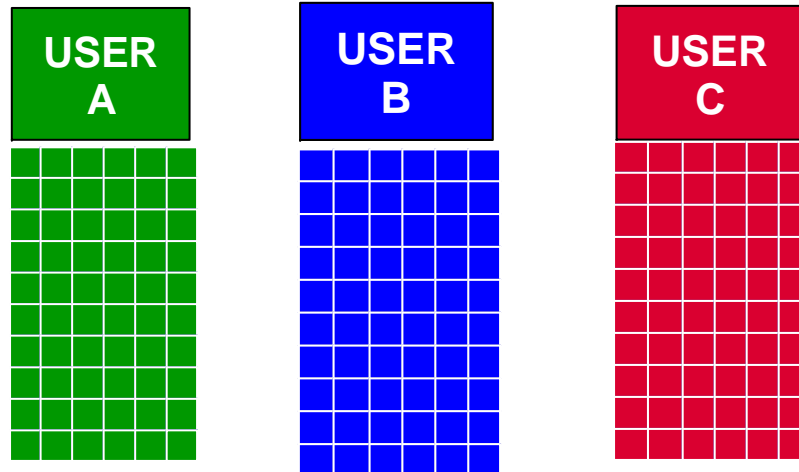
Interpretive Execution Facility - Logical partitions

- PR/SM® enables CP to create virtual machines exactly as LPAR creates partitions, but storage is fixed and contiguous



Hardware Access to Virtual Memory

- SIE uses dynamic address translation to convert virtual addresses to real addresses.



CP Real Memory

- CP provides page, segment, and region tables to SIE
- Page table entries are 'invalid' until initialized by CP

Interpretive Execution Facility

- The only virtualization technology on the market that provides not one, but **two** levels of hardware support for virtualization.
- Level 3+ “pancakes” down to Level 2
- Level 2 for z/VM virtual machines within an LPAR
- Level 1 for LPAR

Virtual I/O

- SIE break – CP examines I/O request
 - ▶ Translates CCW virtual addresses to real addresses
 - ▶ Pins user pages in memory
 - ▶ Looks for harmful operations
 - ▶ Alters minidisk cylinder locations, if required
 - ▶ Inserts device limits whenever possible
 - DEFINE EXTENT for minidisks

- I/O Assist – SIE handles I/O request
 - ▶ Dedicated QDIO devices only
 - OSA and Fibre Channel
 - ▶ No SIE break

CP Commands and Functions

- Commands entered from virtual console
- Diagnose instruction (0x83xx)
- IUCV / APPC instruction (0xB2F0)

- All cause SIE break

Security

What is z/VM System Security

- Authentication: Knowing who is accessing the system or its resources
- Authorization: Ensuring that a user has access only to system resources specifically permitted
- Audit: Knowing who has actually accessed (or failed to access) what resources
- Security is only meaningful in the presence of system integrity!
 - ▶ Integrity prevents bypass of security controls
 - ▶ Audit trail confirms conformance

Authentication

- Based on three basic forms
 - ▶ **What you know: passphrase**
 - ▶ **What you have: security gadget, private key**
 - ▶ **Who you are: biometrics**
- VM uses “What you know” to establish your identity
- Others often used at network or access point boundaries so as to create combinations which provide more security

Authorization

- Native CP authorizations can be supplemented by External Security Manager (ESM), e.g. RACF

- Authorization is based on
 - ▶ who you are: your VM user ID
 - ▶ Unix UID/GID
 - ▶ privilege class
 - ▶ directory authorizations
 - ▶ ESM access control list

- what you know: a password
 - ▶ If minidisks not protected by ESM

Privilege Class

- Each user is assigned one or more privilege classes: A - G
 - ▶ General use is class G
- System administrators have class A, B, C, D, and E
 - ▶ Potential to bypass system integrity and security controls
 - ▶ Do not give to untrusted guests
- Customer can alter CP command privilege classes
- External Security Manager can audit all privileged commands and limit use to specific individuals

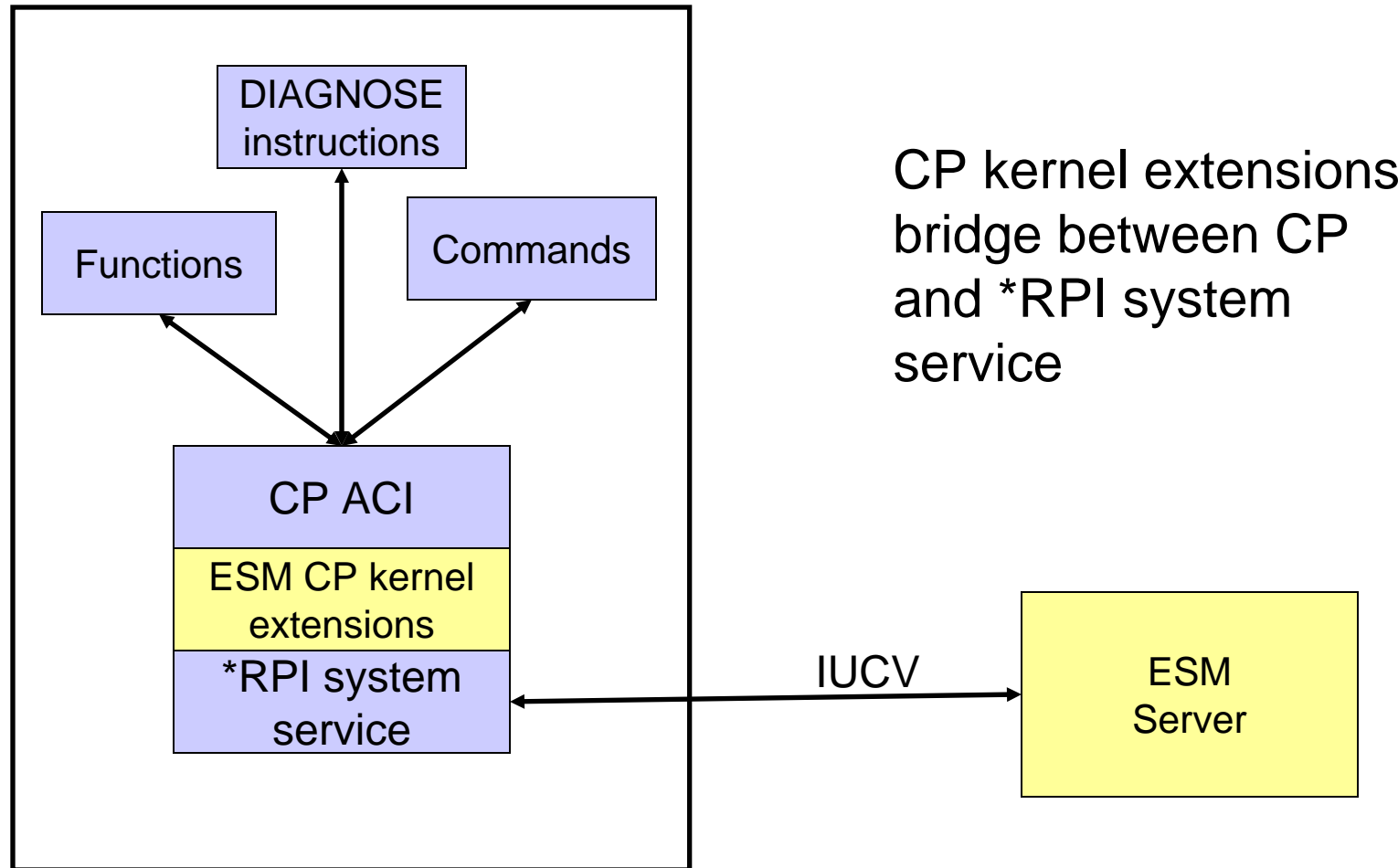
Audit

- CP “journal” records are part of the CP accounting record stream
- Not really very useful as an audit trail
 - ▶ No commands
 - ▶ No diagnose instructions

External Security Manager

- Enhances auditing, authentication, and access controls
- Encrypt user passwords
- Use Access Control List for minidisks instead of minidisk password
- RACF is a feature of z/VM

External Security Manager Structure



Network Security Enhancements for z/VM V5.3



New!

- SSL server support for new levels of Linux SLES9 and RHEL4
- Easier to exclude 40- and 56-bit encryption suites from SSL server
- FTP, Telnet, and SMTP now support RFC-based in-band change from clear-text to secure both z/VM server *and* clients
 - ▶ FTP: RFC 4217
 - ▶ SMTP: RFC 3207
 - ▶ Telnet: TLS-based telnet security draft #6

z/VM RACF Security Server feature FL530



New!

- New name more consistent with z/OS
- Replaces RACF/VM V1.10 (withdrawn from marketing)
- New level numbering scheme consistent with other z/VM features
- New functionality will not be added to prior releases of RACF/VM

z/VM RACF Security Server feature FL530



New!

- **Optional mixed-case 8-character passwords**
- **Mixed-case password phrases up to 100 characters, including blanks**
- **Passwords and phrases can be removed entirely**
- **No longer possible to reset to password to default group name since too many people know the group name**
- **Audit trail can be unloaded in XML format**
- **Remote authentication and audit via new LDAP server and utilities**

LDAP server and utilities



- Enables remote hosts or applications to securely authenticate users against the RACF database on z/VM
 - ▶ E.g. Linux PAM
- Enables central management of z/VM passwords
- Remote audit via LDAP extended operation
- CMS client utilities
 - ▶ Idapadd, Idapsrch, Idapmdfy, Idapmrdn, Idapdlet

IBM Commitment

- Continued investment
 - ▶ Built on almost 40 years of previous investment
- Prompt response to incidents reported to the IBM Support Center
- No public disclosure of IBM System z vulnerabilities
 - ▶ May disclose to individuals or groups that have demonstrated to IBM a legitimate need to know
 - ▶ ResourceLink provides access to more information
- Commitment published in z/VM General Information manual

IBM Commitment: Common Criteria

- Common Criteria ensures
 - ▶ A set of meaningful security functions
 - Access control
 - Audit
 - ▶ Extensive testing of those functions
 - ▶ Effective processes
 - ▶ Good documentation

- Assurance levels 1 through 7
 - ▶ Evaluation by accredited firms
 - ▶ Certification by government agencies
 - ▶ CommonCriteriaPortal.org

IBM Commitment: Common Criteria

- z/VM Version 5.1 completed evaluation
 - ▶ October 2005
 - ▶ Includes CP, TCP/IP stack with telnet, and RACF/VM

- Labeled Security Protection Profile (LSPP)
 - ▶ Mandatory access controls
 - ▶ Security clearances and compartmentalization enforced

- Controlled Access Protection Profile (CAPP)
 - ▶ Discretionary access controls
 - ▶ User- or administrator-controlled access

- Evaluation Assurance Level (EAL) 3+

IBM Commitment: Common Criteria

- z/VM Version 5.3
 - ▶ Statement of Direction for CAPP/LSPP EAL4+
 - ▶ Currently in evaluation
 - ▶ Expect to complete 2Q 2008

- z/VM Version 5.2
 - ▶ Will not be certified
 - ▶ Statement of Direction modified by z/VM V5.3 announcement



Customer Commitments

- Define and deploy a security policy
- Examine audit trails periodically
- Apply recommended service
- Data integrity must be managed by customer
 - ▶ e.g. No multi-write links by virtual servers unless running application that implements data integrity measures such as reserve/release

Summary

- z/VM was designed to host virtual machines
- System z hardware provides facilities used by z/VM to ensure the integrity of the system is maintained
- Backed by 40 years of practical experience in maintaining virtual machines
- IBM commitment
- Customer-defined security policy

Summary

- An external security manager such as RACF/VM is recommended
 - ▶ Privileged command audit trail
 - ▶ Encrypted passwords
 - ▶ ACLs for minidisks instead of passwords
 - ▶ Finer grain of control

- A full discussion of z/VM security and integrity features can be found in publication GM13-0145-01 (April 2005)

<http://www.ibm.com/servers/eserver/zseries/library/techpapers/gm130145.html>

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
 IBMVM@listserv.uark.edu
 LINUX-390@vm.marist.edu

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