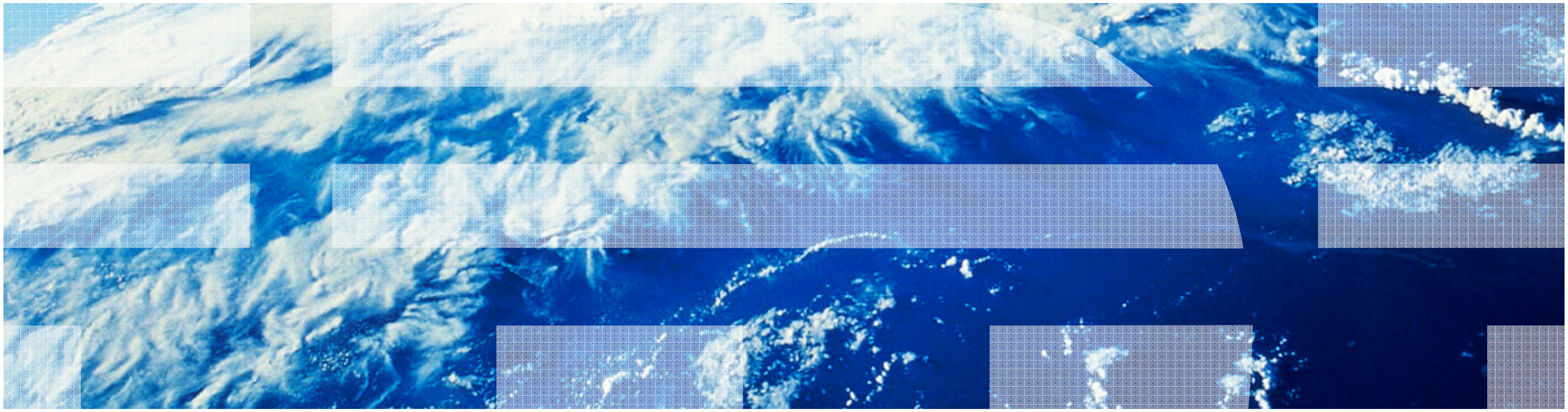
Brian W. Hugenbruch, CISSP
z/VM Security Design and Development
bwhugen@us.ibm.com

z/VM Security and Integrity



Trademarks

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

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* 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.

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "AS IS" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

Any performance data contained in this document was determined in a controlled environment and, therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming or services in your country.

Agenda

- What is Security?
  - How do we apply this to z/VM?
  - Examples and mechanisms

- Auditing

- Certifications

What is Security?

- Access control?
- Cryptography?
- Managing your networks?
- Disaster recovery?
- Conforming to laws and regulations?
- Auditing policies?
- “Guarding what isn’t bolted down?”

Security is:

- a broad topic covering a lot of different disciplines
- subject to increased scrutiny by governments and businesses
- increasingly important in today’s technology discussions

What is Security?

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

What is Security?

- Availability
  - the guarantee that information, systems and resources are accessible to users in a timely manner

What is Security?

Q: How does z/VM work toward high Availability?

1. Extensive testing and debugging over 40+ years as a product have produced a stable environment for "mission-critical" hardware

2. Graceful failure. If something breaks, the errors are isolated and contained.
   - Syntactical and semantic checking of commands
   - Easy to re-IPL
   - Separation of virtual machines

3. Planned outage support and server management through Guest Mobility

4. The goal of five 9's

What is Security?

- Availability
  – the guarantee that information, systems and resources are accessible to users in a timely manner

- Integrity
  – the guarantee that information is accurate, complete and protected from unauthorized modification.

What is Security?

Q: What does Integrity mean to z/VM?

1. The ability of the hypervisor (CP) to operate without interference or harm, intentional or not, from the guest virtual machines

2. The inability of a virtual machine to circumvent system security features and access controls

3. The ability of the hypervisor to protect virtual machines from each other

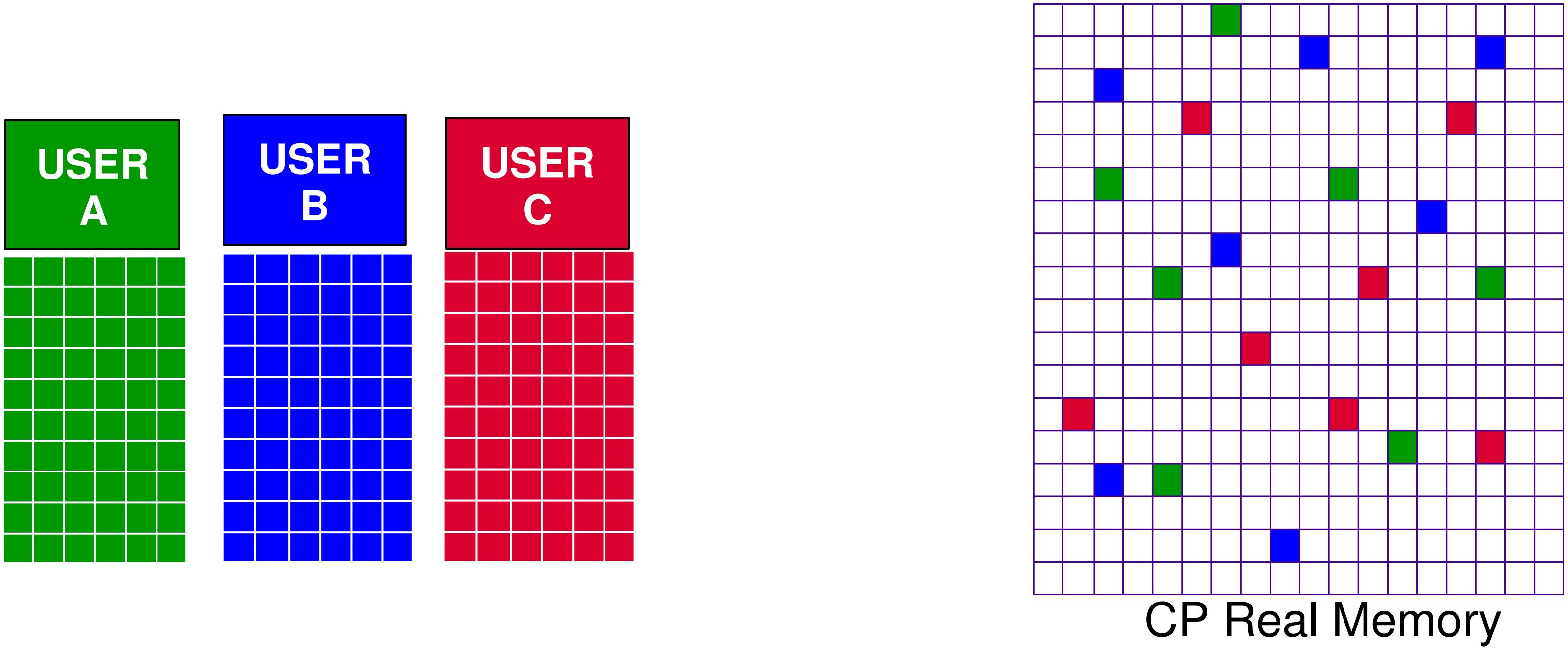
Q: So, how do we accomplish all this?

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
  - Certain program interrupts
- SIE runs until interception condition raised

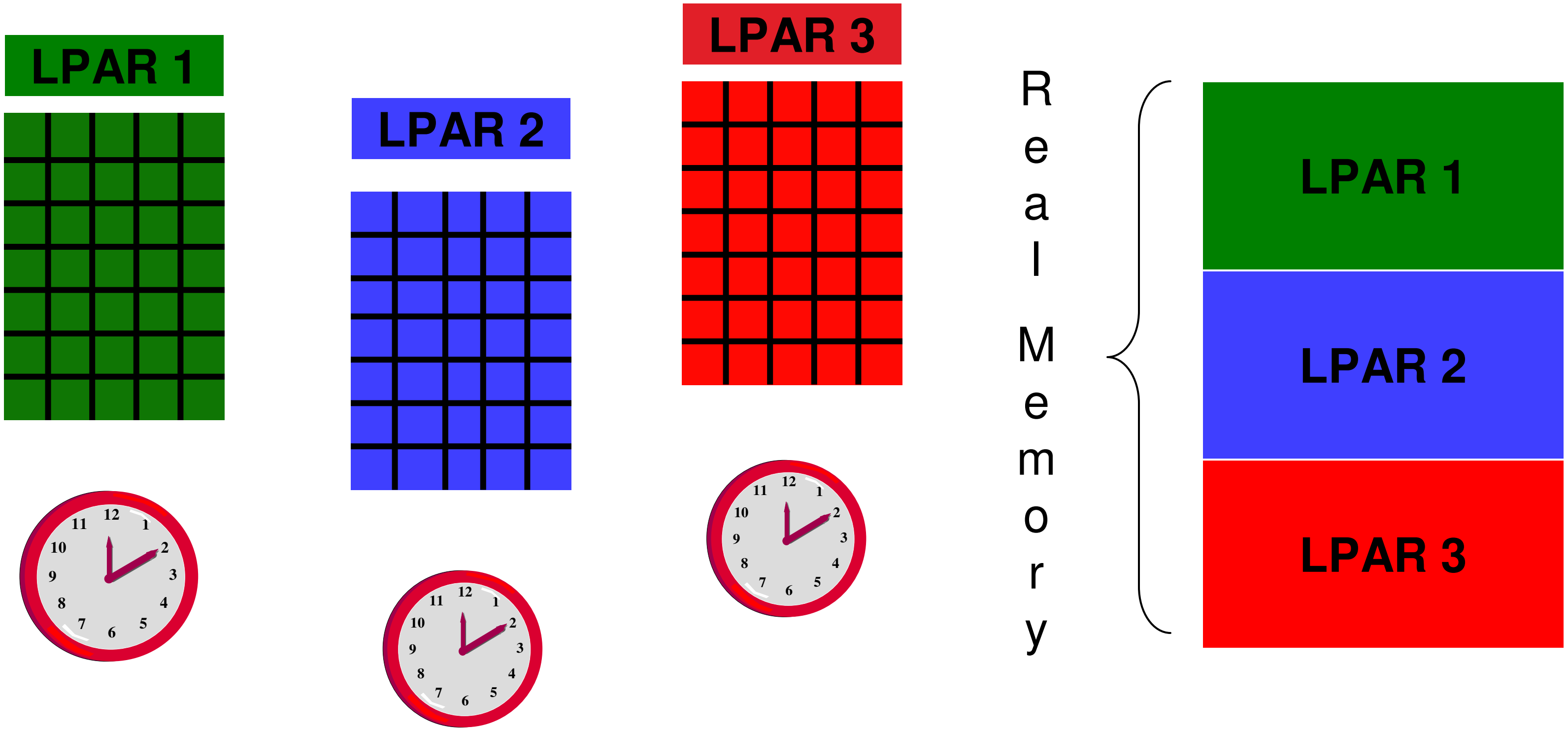
Hardware Access to Virtual Memory

- SIE uses dynamic address translation to convert virtual addresses to real addresses.
- CP provides page, segment, and region tables to SIE
- Page table entries are ‘invalid’ until initialized by CP



Interpretive Execution Facility

- To a virtual machine, “real” is a virtual reality created by the underlying *hypervisor*
- “Soft” and “hard” virtualization



Interpretive Execution Facility

- Provides not one, but two levels of hardware support for virtualization

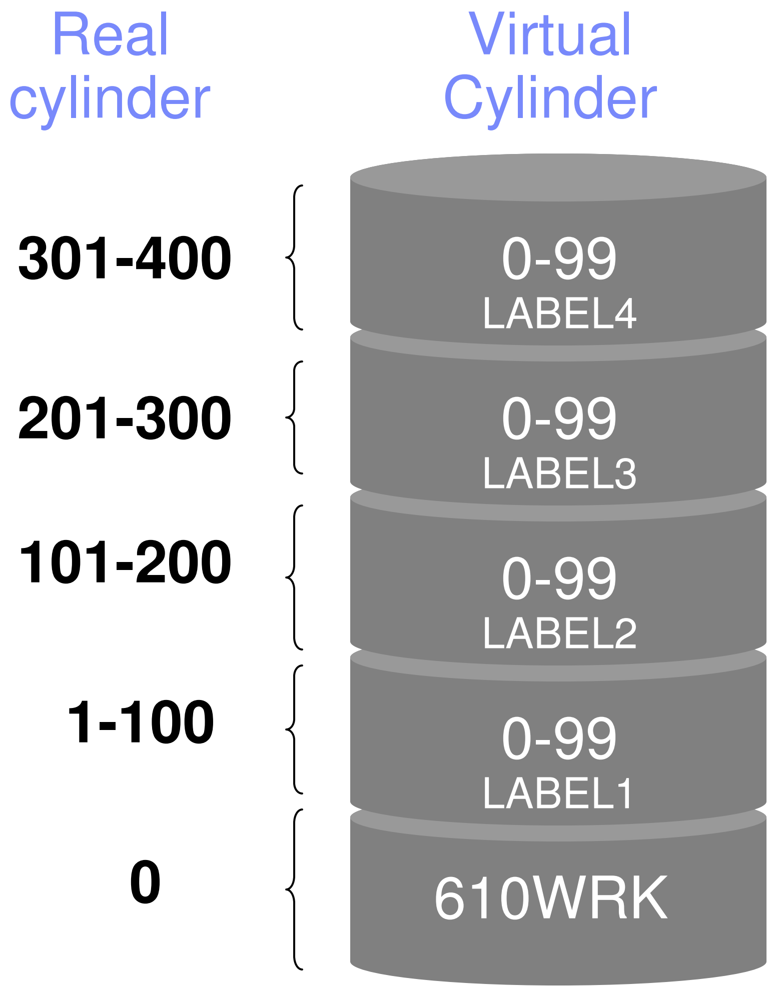
- Level 3+ “pancakes” down to Level 2
  - SIE is always used to run a virtual machine, no matter how “high up”

- Level 2 runs a virtual machine within a z/VM LPAR

- Level 1 runs the 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 Hardware Assist

- Interpretive Execution Facility handles I/O request
  - No SIE break, so no involvement of CP
  - CP and hardware share address tables

- Dedicated QDIO devices only
  - OSA and Fibre Channel

Security and Integrity

- System security is only meaningful in the presence of system integrity!
  - Audit trail confirms conformance
  - Integrity prevents bypass of security controls

What is Security?

- Availability
  - the guarantee that information, systems and resources are accessible to users in a timely manner
- Integrity
  - the guarantee that information is accurate, complete and protected from unauthorized modification.
- Confidentiality
  - the guarantee that information is not disclosed to unauthorized individuals, programs, or processes.

What is Security?

Q: How do we manage Confidentiality in z/VM?

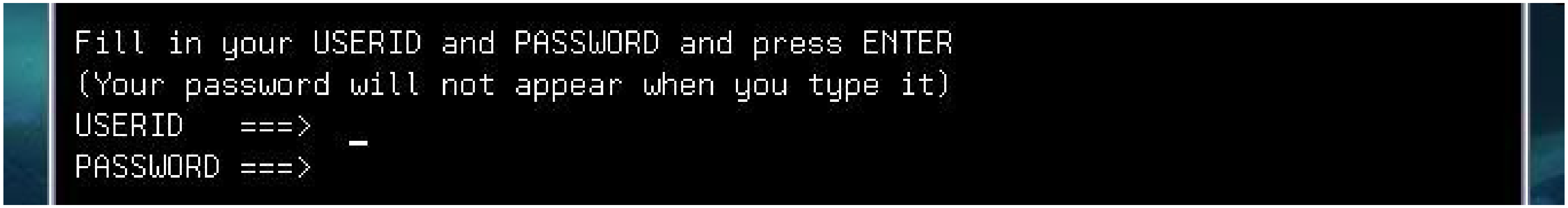
A: In three words:

- **A**uthentication
- **A**uthorization
- **A**uditing

What is Security?

Authentication

- Identification is, for example, asking for a userid or log-on name



```
Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>
PASSWORD ===>
```

- **Authentication** is the confirmation of the identity presented – in other words, guaranteeing that you are who you **say** you are

What is Security?

Authentication

- Several ways of authenticating a user:
  - what a person **has** (digital certificate, swipe card)
  - what a person **knows** (password, passphrase or PIN)
  - what a person **is** (fingerprints, biometric data)

- z/VM virtual machines and mechanisms use a password and/or a passphrase (“what you know”)
  - Logon processing
  - FTP
  - REXEC
  - NFS

Authentication in z/VM

- About your passwords …
  - up to 8 alphanumeric characters
  - stored in clear text in USER DIRECT
  - obfuscated in the object directory
  - an **External Security Manager (ESM)** provides for secure, encrypted passwords

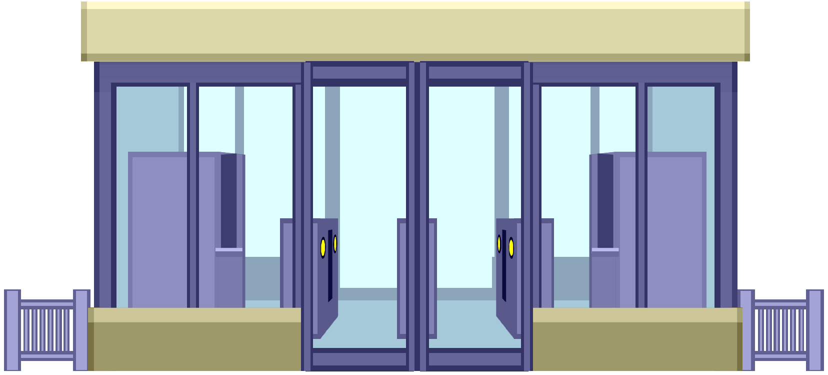
- An ESM is required to use password phrase support in z/VM:
  - up to 100 characters
  - case sensitive
  - special characters and blanks

What is Security?

Authorization

- A user, *once authenticated*, should only have access to system resources which are within scope of responsibility or have been specifically granted

- This applies to
  - **commands**,
  - **interfaces**,
  - **devices**,
  - and **data**

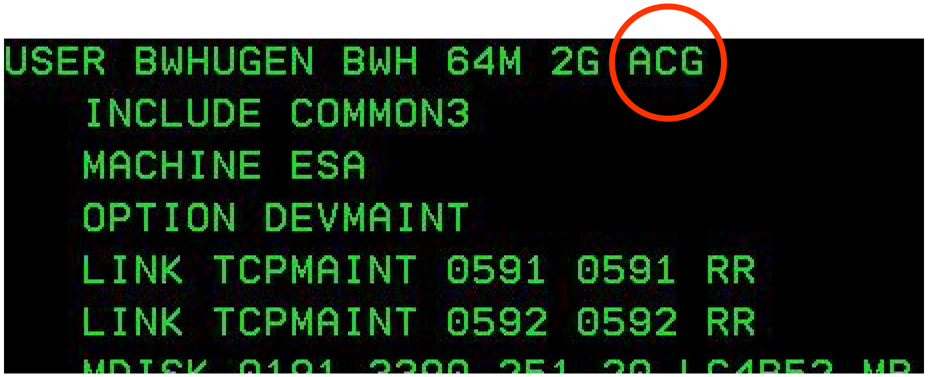


What is Security?

Authorization

- The privilege class is your first line of protection

- Defines what commands and DIAGNOSE functions the userid can use



```
USER BWHUGEN BWH 64M 2G ACG
   INCLUDE COMMON3
   MACHINE ESA
   OPTION DEVMAINT
   LINK TCPMAINT 0591 0591 RR
   LINK TCPMAINT 0592 0592 RR
   MDISK 0191 3390 251 20 LC4RE2 MR
```

- Each user is assigned one or more privilege classes
  - “General use” is class G
  - More power given to “trusted users”
  - Make your own

- Using the word “secure” demands a lot of your system, software, and hardware. But the essentials all exist inside of z/VM, when properly configured.

- But what happens when we ask you to prove it?

Auditing z/VM

- Auditing is the assessment of a system’s internal control
  - Provides **proof** that your system is being operated according to your security policy

- It is the **most important** data asset
  - How do you know that your business data has not had unauthorized updates?
  - How do you **know** if someone has accessed data for which they were unauthorized?
  - How do you tell **which** userid issued that SHUTDOWN command?

Auditing z/VM

- CP “journal” records are part of the CP accounting record stream

- It’s a start, but … it’s often not enough
  - No commands listed
  - No diagnose instructions listed

- Instead, use an **External Security Manager** with z/VM
  - **Full record** of any command or system interface
  - **Enhances** auditing, authentication, and access controls
  - **Encrypt** user passwords
  - Use **A**ccess **C**ontrol **L**ist for minidisks instead of minidisk password

z/VM RACF Security Server

- Pre-installed optional feature of z/VM
  - Priced separately from the main product
  - Competes with other security products

- Long-lived (1986)

- Trusted brand
  - Shared heritage with flagship z/OS version
  - In business since 1976

ESM Security Controls

- Mixed-case passwords and longer password phrases
- Virtual Switches and Guest LANs
- VLANs
- Minidisks
- Shared memory
- Shared virtual machines
- Spool files

- Terminals (restricted login)
- Multiple security zones (projects)
- Security clearances within zones
- Certain commands (e.g. STORE HOST)
- Control Program interfaces
- Full audit: interface, command, virtual machine

- Can be configured to serve as an LDAP back-end for identity management

IBM Commitment

- z/VM is a long-lived product
  - Built on 40+ years of previous investment (CP/67)
  - Thoroughly tested and fully supported
  - Formal Security and Integrity Statement

- 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

- Commitment published in z/VM General Information manual

But don’t take our word for it.

- **Certifications** make **assurances** about the stability and reliability of a product

- Outside groups issue (and vouch for) certifications
  - ANSI: “American National Standards Institute”
  - ISO/IEC: “International Organization for Standardization” / “International Electrotechnic Commission”

- Works for software processes …
  - Software Lifecycle Management: ISO/IEC 12207

- … security mechanisms …
  - Common Criteria Certification: ISO/IEC 15408

- … and even people.
  - Brian W. Hugenbruch, CISSP: ISO/IEC 17204

Common Criteria

- An international standard, ISO 15408 (www.CommonCriteriaPortal.org), comprised of two distinct and equally important parts:

Security Target: *The Claim*

Can be a standardized Protection Profile

CAPP, LSPP, OSPP, SKPP, MLOSPP, …

… or Enumerated functional specifications

E.g., PR/SM evaluations

Evaluation Assurance Level (**EAL**): *The Proof*

1 = The back-of-envelope sketch

2-6 = More and more comprehensive design, test

7 = Mathematical proof with exhaustive tests

- Security certifications ensure:
  - – A set of meaningful security functions
    - Access control
    - Auditing
  - – Extensive testing of those functions
  - – Effective processes
  - – Good documentation

Certifications

Some examples of Evaluation Assurance Levels (EALs):

PR/SM for z10 EC GA2 and z10 BC	EAL 5
zVM 5.1	EAL 3+ with LSPP and CAPP
zVM 5.3	EAL 4+ with LSPP and CAPP
Red Hat Linux (RHEL 5)	EAL 4+ with LSPP and CAPP
SuSE Linux (SLES 10)	EAL 4+ with CAPP

- “Plus” (+) means you can fix a security problem in the field
- Higher assurance level does not necessarily indicate “more security”

Certifications

A **Protection Profile** defines a set of required functions

- Controlled Access Protection Profile (CAPP)
  - Discretionary access controls
  - “I choose to give you access”
  - User- or administrator-controlled access
- Labeled Security Protection Profile (LSPP)
  - Mandatory access controls (MAC)
  - System overrides user
  - Security clearances and compartmentalization enforced:

    “No read up, no write down.
- Operating System Protection Profile (OSPP)
  - Tailored more closely to modern software
  - Has optional extensions for virtualization and labeled security

- Products may define Security Targets without using a standardized profile
- Make sure you understand the claims, either way

We can only show you the door.

The most secure product in the world can be breached if not configured properly.

Take steps to ensure that their virtual machines are deployed securely and stay secure:

- Define and deploy a security policy
- Examine audit trails periodically
- Apply recommended service
- Use an ESM
- Manage data integrity carefully
- Don’t grant extra privileges
- Don’t keep default passwords, or share passwords between userids!
  - Use LOGONBY for privileged users
  - Trusted Servers LOGONBY or AUTOONLY

Summary

- Security is a broad field, covering many disciplines and areas of relevance
  - Availability, Integrity, Confidentiality
  - Authentication, authorization, auditing

- 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

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

For more information …

Speaker: Brian W. Hugenbruch, CISSP

- Web: http://www.vm.ibm.com/devpages/hugenbru
- Mail: bwhugen at us dot ibm dot com

On the web:

- z/VM Security resources: http://www.VM.ibm.com/security
- z/VM Secure Configuration Guide: http://publibz.boulder.ibm.com/epubs/pdf/hcss0b30.pdf
- System z Security: http://www.ibm.com/systems/z/advantages/security/
- Redbook: z/VM Security, SG24-7471

With thanks to:

- Alan Altmark, IBM Lab Services

Dank u
Dutch

Merci
French

Спасибо
Russian

Gracias
Spanish

شكراً
Arabic

감사합니다
Korean

Tack så mycket
Swedish

धन्यवाद
Hindi

תודה רבה
Hebrew

谢谢
Chinese

Obrigado
Brazilian Portuguese

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

ขอบคุณ
Thai

děkuji
Czech

go raibh maith agat
Gaelic