

What It Means to Measure Your z/VM Security

Or, using standards, certifications, auditing, and security-relevant service to maintain a healthy and happy hypervisor

Brian W. Hugenbruch, CISSP

IBM Z Security for Virtualization and Cloud

bwhugen@us.ibm.com



@Bwhugen



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:

*, IBM Systems, IBM System z10®, IBM System Storage®, IBM System Storage DS®, IBM BladeCenter®, IBM System z®, IBM System p®, IBM System i®, IBM System x®, IBM IntelliStation®, IBM Power Architecture®, IBM SureOne®, IBM Power Systems™, POWER®, POWER6®, POWER7®, POWER8®, Power®, IBM z/OS®, IBM AIX®, IBM i, IBM z/VSE®, IBM z/VM®, IBM i5/OS®, IBM zEnterprise®, Smarter Planet™, Storwize®, XIV®, PureSystems™, PureFlex™, PureApplication™, IBM Flex System™, Smarter Storage

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.

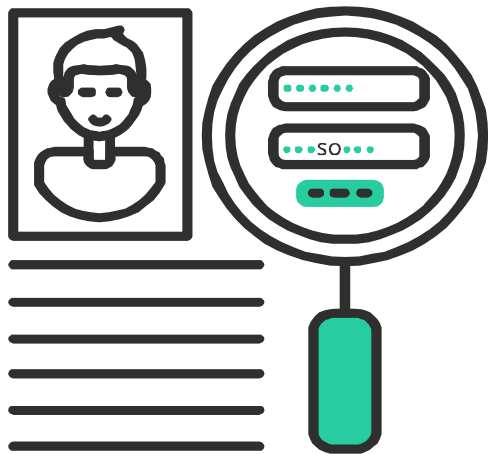
Any performance data contained in this document was determined in a controlled environment and, therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

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? (*No, seriously ... what is it?*)
 - And how do you measure it?
- **Certification:** Measuring the Base Product
- **Compliance:** Measuring the Configuration
- **Changes:** Measuring Patches and Service
- **Conclusion**

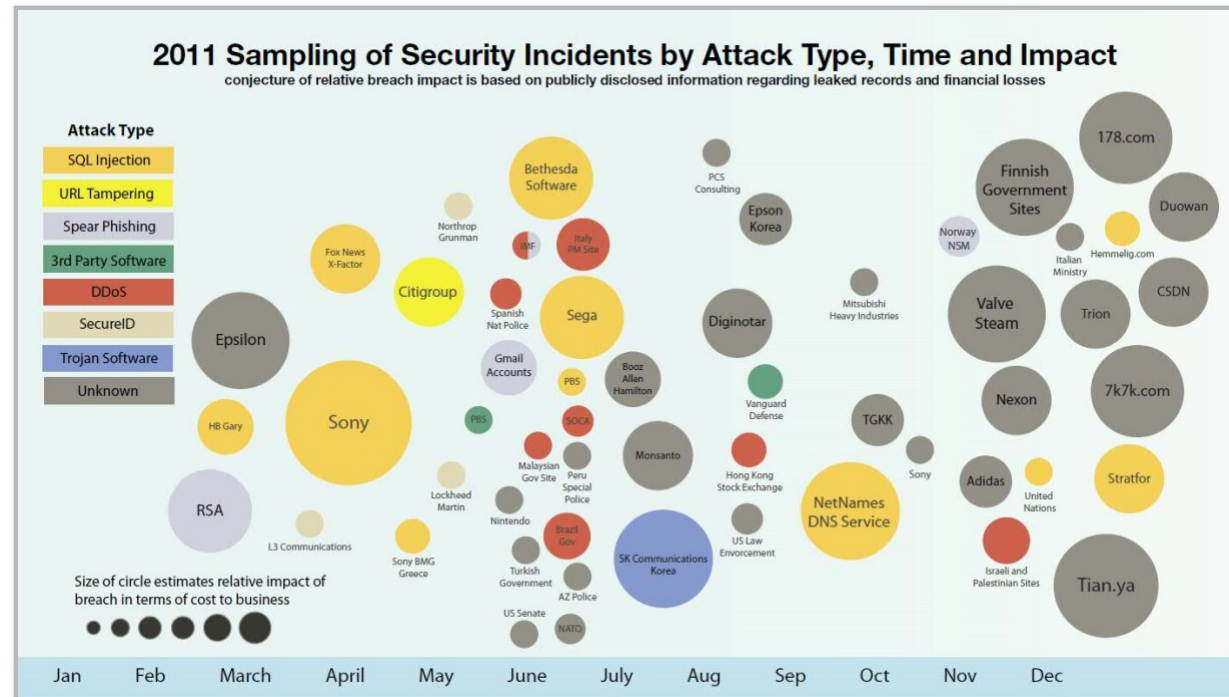




What is Security?

IBM X-Force declared 2011: “Year of the Security Breach”

- SQL injections, Certificate authority compromises (DigiNotar)
- Denial-of-Service attacks
- Social “hacktivism”
- “Advanced Persistent Threats”



... then there was a year after 2011.

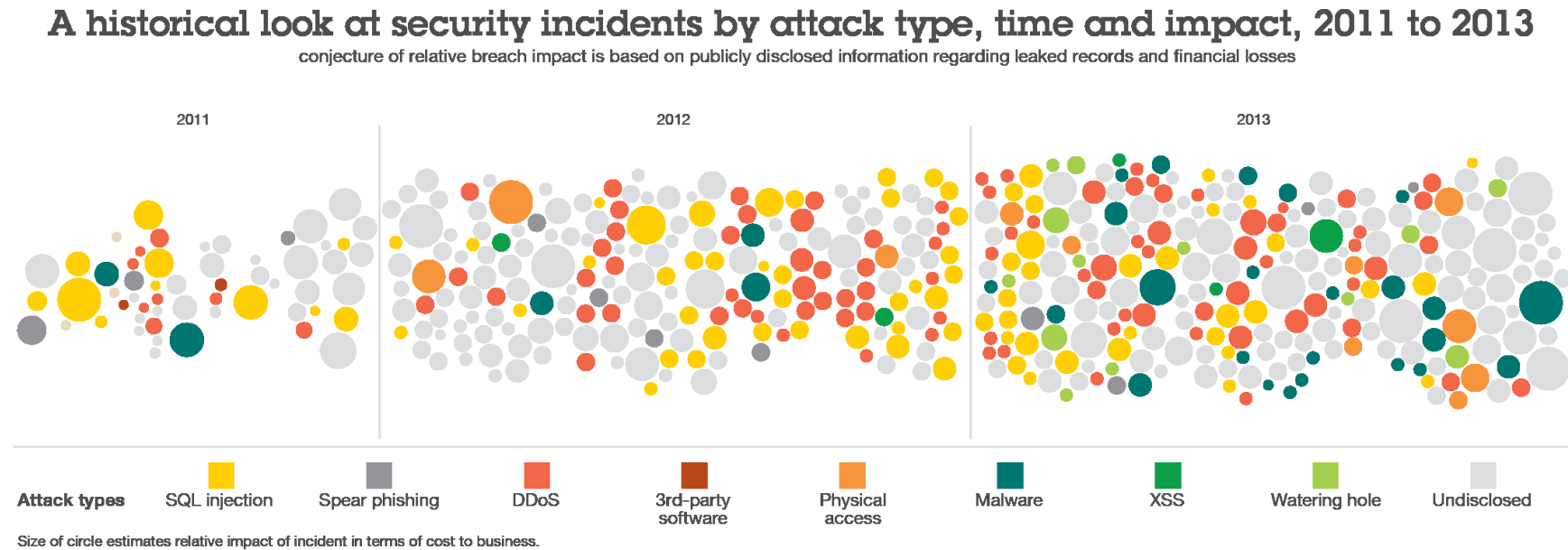
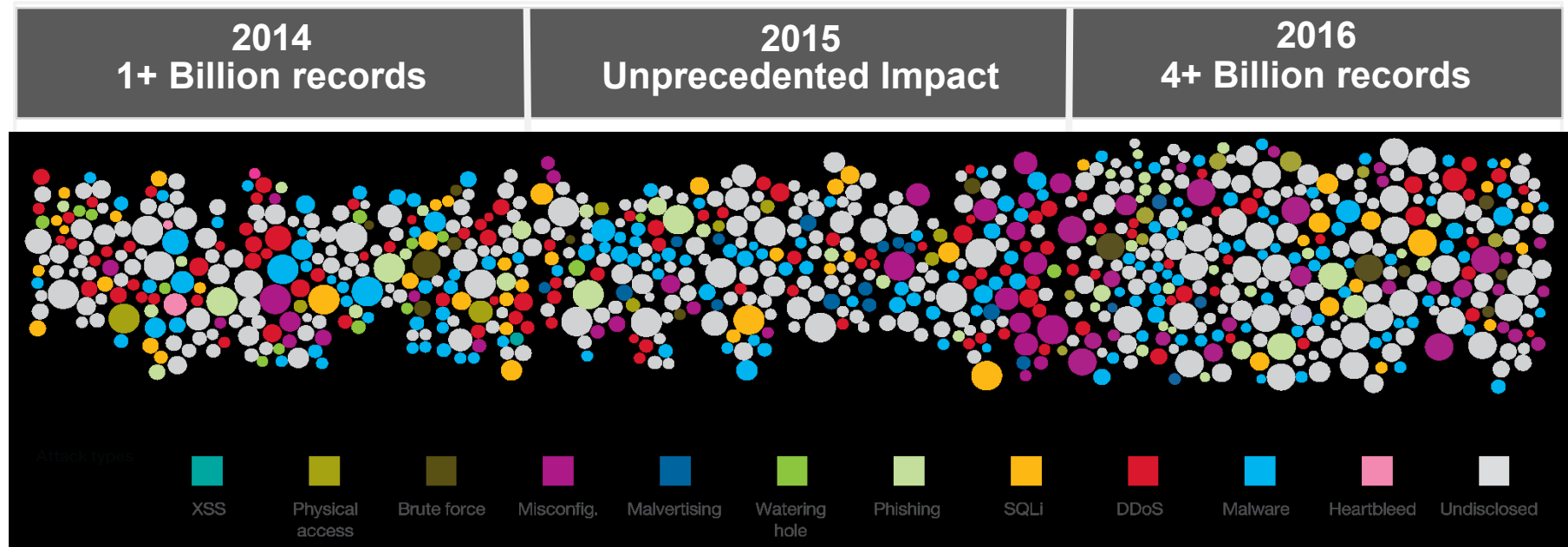


Figure 1. A historical look at security incidents by attack type, time and impact, 2011 to 2013

Source: IBM X-Force® Research and Development

Today's threats continue to rise in numbers and scale

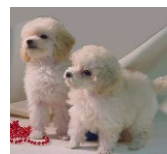


average time to identify data breach

201 days

average cost of a U.S. data breach

\$7M

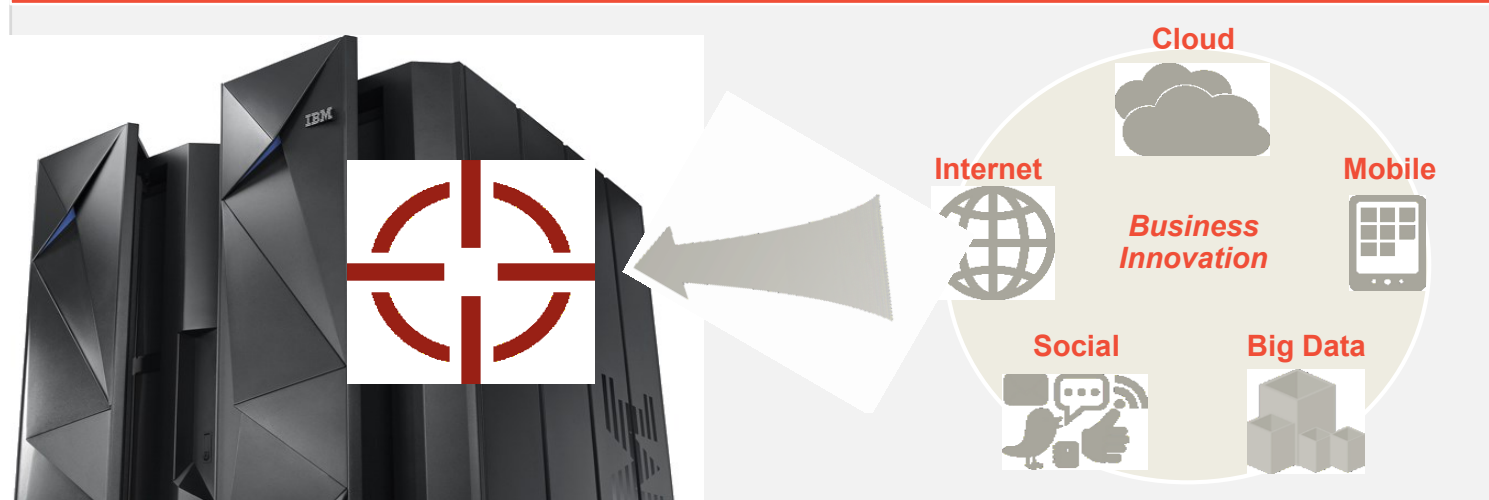


The increasingly desirable target of non-x86 architecture

80 %
of all active code
runs on the mainframe

80 %
of enterprise data is
housed on the mainframe

Today's technologies are eliminating "mainframe isolation"



Source: 2013 IBM zEnterprise Technology Summit

IBM's Commitment to Security & Integrity

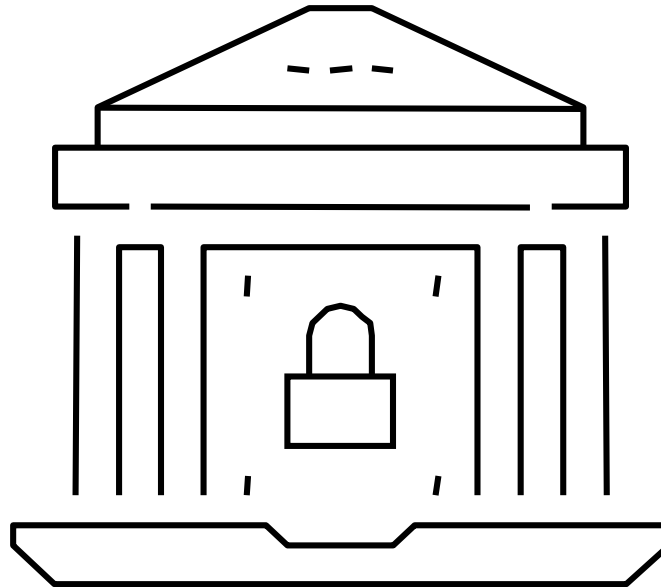


**First issued in 1973 &
Reaffirmed in 2007**

IBM's long-term commitment to System Integrity is unique in the industry, and forms the basis of z/OS & z/VM industry leadership in system security

- “System Integrity” is defined as the inability of any program not authorized by a mechanism under the installation’s control to circumvent or disable z/OS or z/VM Security Controls
- In the event that an IBM System Integrity problem is reported, IBM will always take action to resolve it.
- IBM’s commitment extends to design, development and test practices. Including the creation of the *z Systems Center for Secure Engineering* to provide additional security focused testing and scrutiny.
- The [IBM Z Security Portal](http://www.ibm.com/systems/z/os/zos/features/racf/zos_integrity_statement.html) informs clients about the latest security and system integrity service to help keep their enterprise up to date

I know, let's use some *Security!*



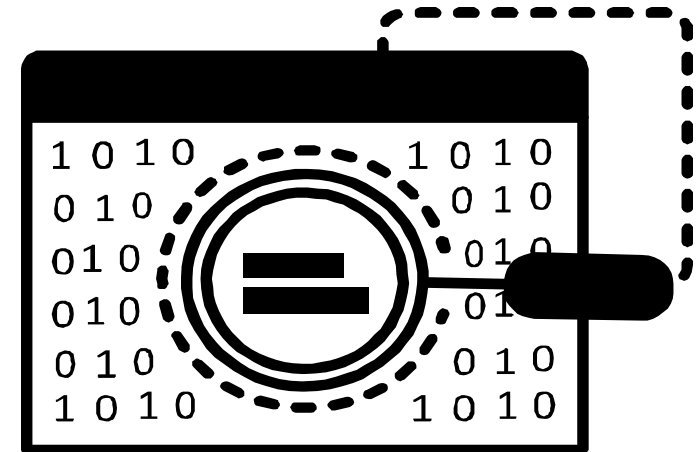
■ “Well, that’s just RACF, isn’t it?”

Information security is a set of mechanisms
through which
the **availability, integrity, and confidentiality** of
assets (e.g., resources, services, and data)
are preserved and protected
against potential **threats**.

What are the Threats to a virtualized environment?

**(An example list from the PCI DSS v2 standard)*

1. Vulnerabilities in the Physical Environment Apply in a Virtual Environment
2. Hypervisor Creates a New Attack Surface
3. Increased Complexity of Virtualized Systems and Networks
4. More than One Function per Physical System
5. Mixing VMs of Different Trust Levels
6. Lack of Separation of Duties
7. Dormant Virtual Machines
8. VM Images and Snapshots
9. Immaturity of Monitoring Solutions
10. Information Leakage between Virtual Network Segments
11. Information Leakage between Virtual Components



Assessing Risk in Virtual Environments

(An example list from the PCI DSS v2 standard)

- Define the environment
 - Components, physical site details, primary functions and owners,
 - visibility into and between components, traffic flow between components,
 - intra-host communication and data flow, out of band communication channels,
 - management interfaces, hypervisors access mechanisms, virtual and physical hardware components, and
 - the number of types of virtual components on each host (segmentation between components and hosts, functions, security levels, etc.).
 - **ProTip: Draw a picture of where the card data flows**
 - **A Requirement in PCI DSS v3!**
- Identify threats
- Identify vulnerabilities
- Evaluate and address risk

It's not always easy to determine a threat.

- Does a Type 80 Event 1 SMF Record (for a successful logon) count as a security risk?
 - What if the owner of **BWHUGEN** was on vacation that week?
 - What if the password was changed recently? (What if it wasn't?)
- How many products on the market are rated EAL 4 under the Common Criteria? Do they all really have the same security?
 - Is that the “out of the box” security? And what are the restrictions?
 - What's the Specific Coverage Metric* (SCM) cover on a system?
- Even if you prove the security of a system, what happens when a PTF is rolled out?



*the percentage of tested components, relative to all components under review.

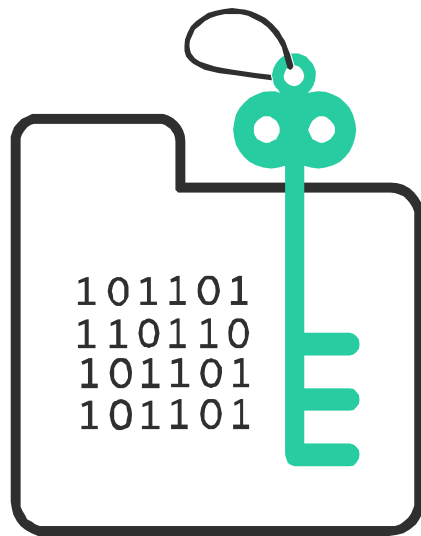
This is the thesis statement.

- If there is one attribute of security to which everyone can agree, it is this:

Frphevgl vf nyjnlf ba gur zbir.

Security is always on the move.

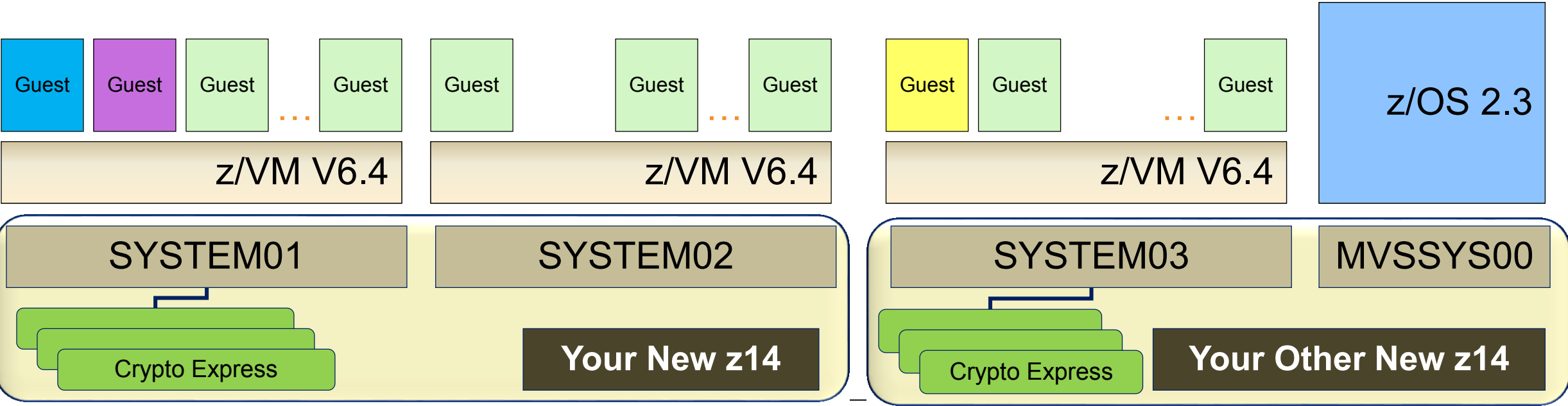
- Understanding the **capabilities of a base product**, the **requirements of a security policy**, the **requisites of monitoring**, and the **impact of service** will help us to measure security over time.



Measuring the Product



It's 22:00h. Do you know where your data is?



IBM's z/VM System Integrity Statement

(a small portion)

z/VM System Integrity Definition

The z/VM control program system integrity is the inability of any program running in a virtual machine not authorized by a z/VM control program mechanism under the customer's control or a guest operating system mechanism under the customer's control to:

- Circumvent or disable the control program real or auxiliary storage protection.
- Access a resource protected by RACF. Resources protected by RACF include virtual machines, minidisks, and terminals.
- Access a control program password-protected resource.
- Obtain control in real supervisor state or with privilege class authority or directory capabilities greater than those it was assigned.
- Circumvent the system integrity of any guest operating system that itself has system integrity as the result of an operation by any z/VM control program facility.

- Read the full statement at: <http://www.vm.ibm.com/security/zvminteg.html>

“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

z/VM Security Certifications

V6.4 Statements of Direction: 25 October 2016

z/VM Level	Common Criteria	FIPS 140-2
z/VM 6.4	Formally Started http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/in-corso-di-valutazione	Formally Started https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List
z/VM 6.3 (EOS YE17)	OSPP with Labeled Security and Virtualization at EAL 4+ <ul style="list-style-type: none"> • BSI-DSZ-CC-0903 • Valid through March 2020. 	FIPS 140-2 L1
z/VM 6.1 (Out of service)	OSPP with Labeled Security and Virtualization at EAL 4+ <ul style="list-style-type: none"> • BSI-DSZ-CC-0752 	FIPS 140-2 L1
z/VM 5.3 (Out of service)	CAPP/LSPP at EAL 4+	n/a

z/VM releases not listed are "designed to conform to the standards of each security evaluation."



TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

What is the Common Criteria?

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

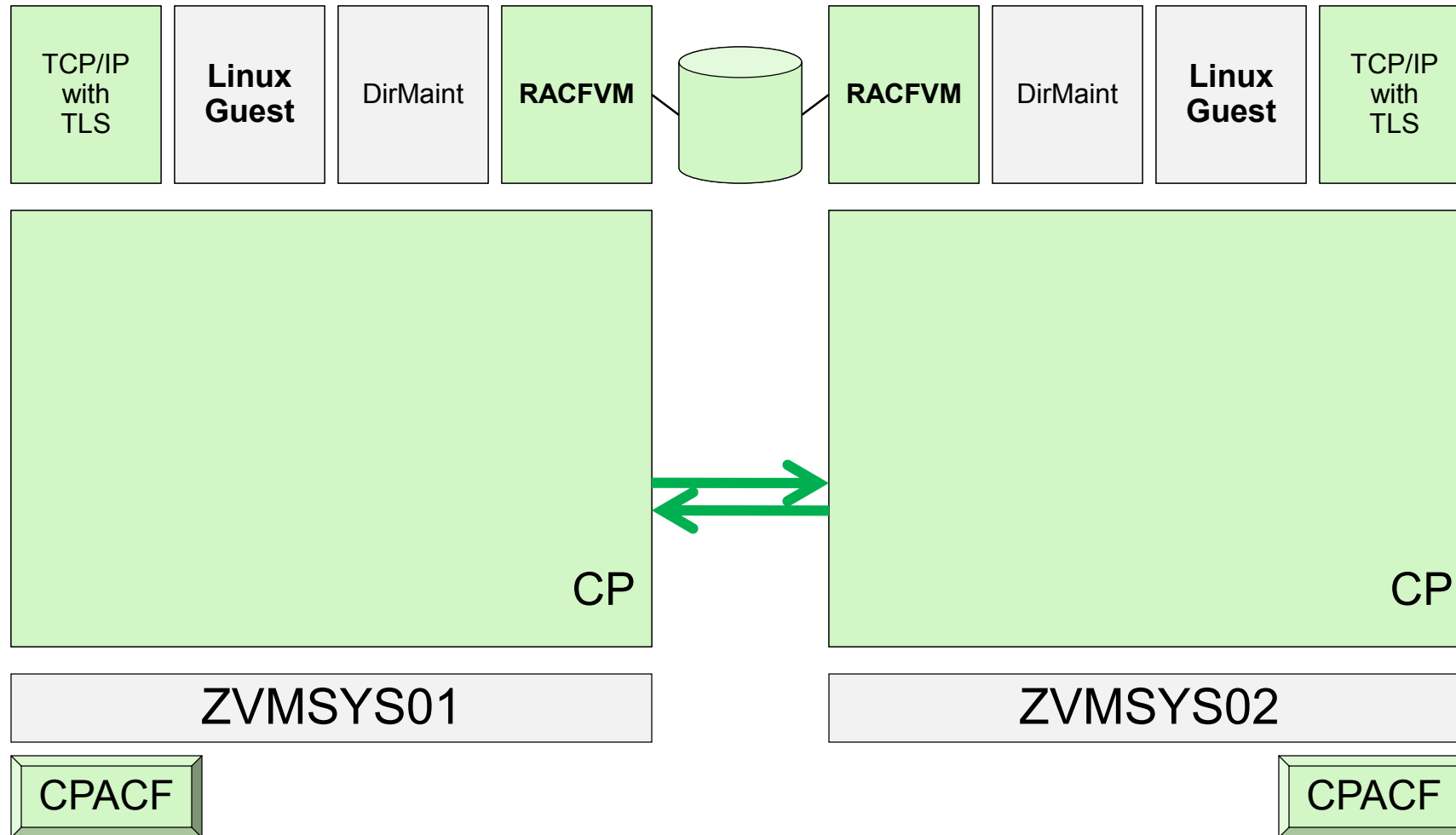
–**Security Target:** What claims are we making?

- Standardized checklists are called Protection Profiles
- CAPP, LSPP, OSPP, SVPP ...
- Can also write your own (e.g., PR/SM)

–**Assurance Level:** How much proof did we provide for these claims?

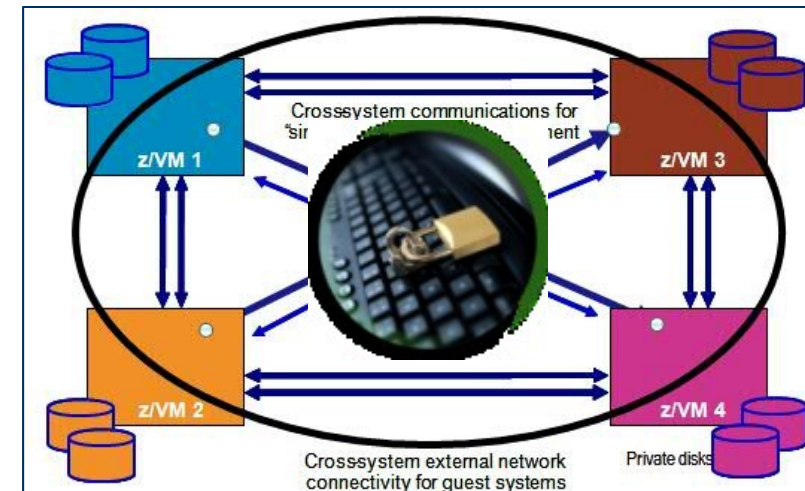
- EAL 1 (lowest) to EAL 7 (highest) – EAL 4 is the most common for this industry
- This number is meaningless without an understanding of the Security Target.

The Common Criteria evaluated configuration of z/VM



Infrastructure Security with RACF for z/VM

- RACF Security Server is a priced feature of z/VM
- A **requirement** for meeting today's enterprise security requirements
- RACF enhances z/VM by providing:
 - Extensive **auditing** of system events
 - **Strong Encryption** of passwords and password phrases
 - **Control** of privileged system commands
 - Extensibility in z/VM environments
 - **clustered** through Single System Image
 - Controls on password policies, access rights, and security management
 - Security Labeling and Zoning for **multi-tenancy** within a single LPAR (or across a cluster)
- RACF for z/VM is an **integral component** of z/VM's *Common Criteria evaluations (OSPP-LS at EAL 4+)*

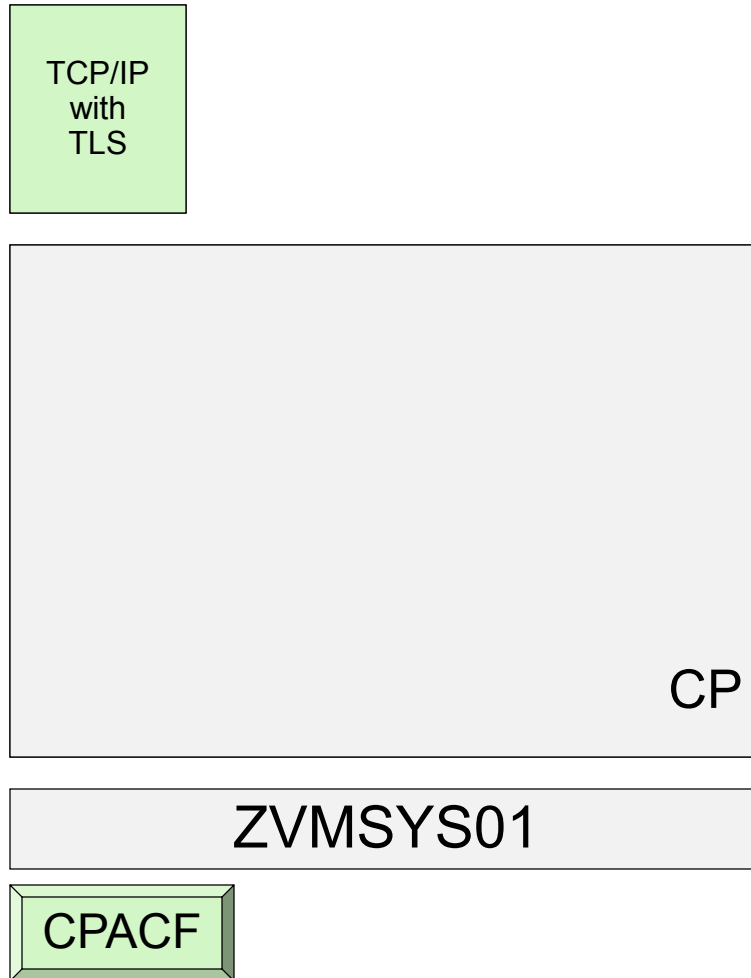


z/VM Security Certification Discussion (CC)

- Only **certain parts of z/VM** are evaluated
 - z/VM Control Program and RACF for z/VM
 - z/VM TCP/IP, Telnet and the TLS/SSL Server
 - **z/VM Single System Image feature** **new to the z/VM 6.3 evaluation**
 - Supports a cluster of "1 to n" z/VM systems
- **A particular code level** of these parts is required
 - See the latest edition of the *z/VM Secure Configuration Guide*
 - Lists associated service to apply
- **A particular configuration** of that code level is also required
 - System Configuration Features, OPERATOR security, device management
 - TLS ciphers and encryption requirements
 - Specific RACF/VM password policies, auditing rules, and command controls
 - Again, refer to the latest edition of the *z/VM Secure Configuration Guide*
 - *Extra rules included for multitenancy compliance (labeled security)*
- Security-related service can be applied without invalidating configuration
 - EAL4 “+” – “Flaw Remediation”
 - No claims made about other service –includes new hardware support



The FIPS 140-2 evaluated configuration of z/VM



▪ **z/VM System SSL**

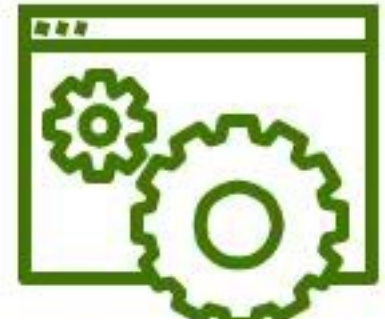
- Instantiated on a per-VM basis
- No access to Crypto Express measured
- Does access CPACF
- No direct CP involvement

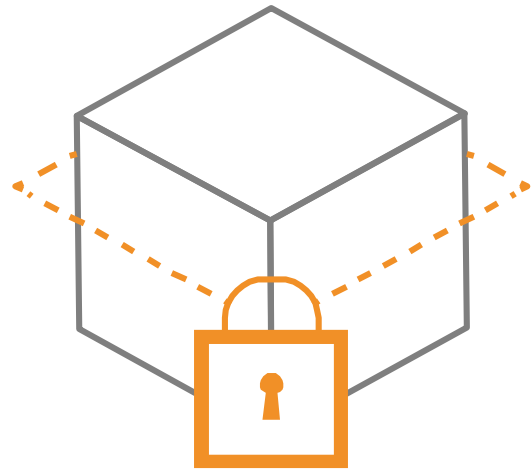
▪ The FIPS evaluation:

- Validates algorithms
- Validates key sizes
- Validates integrity checking
- Validates entropy
- Validates access
- Power-On Self Testing
- "FIPS-mode" certificate database

... but certifications aren't “enough.”

- All certifications for information security will require a particular configuration.
 - This includes z/VM Common Criteria evaluation (OSPP at EAL 4+)
 - ... and z/VM's FIPS 140-2 validation (for secure connectivity)
- **Your needs may vary**, based upon your security policy
 - Based on the needs of a government, industry, or company
 - Additional software (e.g. DirMaint) needs to be considered
 - The Common Criteria configuration is **a good starting point**.
 - “Knowing the path” vs. “walking the path.”
- **Virtualization security will always require some basics:**
 - Isolation of hosted guests
 - Confidentiality of data on the system
 - Protection of privileged hypervisor commands and operations
 - Securing connectivity to the hypervisor layer
 - TCP/IP connectivity and virtual networking
 - Multi-tenancy and “security zones” – especially for Cloud Service Providers!
 - **Auditing of security-relevant operations**





Measuring the Configuration

- Certifications only tell the beginning of the story
 - It declares “the toolbox is full.”
 - Do you know how to use those tools?
 - What are you building?



- Measure twice; cut once

So what are you measuring? Well, it depends!

(“Units, units, units!”)

- Know your company’s security policy
 - Security begins at the management level
 - Security isn’t always relative to the number of people on staff.

- Know your industry standards and local laws
 - Does local policy already account for these?
 - PCI DSS, SOX, HIPAA, FIPS, APEC, OECD...?

- Know how to prove it
 - Not all questions come from the checklist, but that’s not a bad place to start
 - Remember that not every security issue shows up as a “failure” in the audit logs

Recommendations For Virtual Environments

(An example list from the PCI DSS v3 standard)

- 4.1.1 – Evaluate risks associated with virtual technologies
- 4.1.2 – Understand impact of Virtualization to scope of the CDE
- 4.1.3 – Restrict physical access
- **4.1.4 – Implement defense in depth**
- **4.1.5 – Isolate security functions**
- **4.1.6 – Enforce least privilege and separation of duties**
- 4.1.7 – Evaluate hypervisor technologies
- **4.1.8 – Harden the hypervisor**
- **4.1.9 – Harden virtual machines and other components**
- **4.1.10 – Define appropriate use of management tools**
- **4.1.11 – Recognize the dynamic nature of virtual machines**
- **4.1.12 – Evaluate virtualized network security features**
- 4.1.13 – Clearly define all hosted virtual services
- 4.1.14 – Understand the technology

So let's take a look at a couple of **examples**:

An example **regulation**,

The security **consideration** involved,

The z/VM **applicability**,

And **what commands** might come up in the process

Example: PCI DSS and Default Passwords

2.1 Always change vendor-supplied defaults **before** installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

2.1 Choose a sample of system components, and attempt to log on (with system administrator help) to the devices using default vendor-supplied accounts and passwords, to verify that default accounts and passwords have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)

- Have you changed the default passwords in your z/VM User Directory?
- Have the virtual machines associated with unused services been changed to NOLOG?
- Are you using the PROTECTED attribute (starting in z/VM V6.2) for service virtual machines?

Example: PCI DSS and Default Passwords

▪ User Attribute: **PROTECTED**

- Shields user access from being revoked due to logon failures, inactivity or unsuccessful access attempts ... via any method that uses a supplied password (logon, FTP ...)
- Service machines are a good candidate for this attribute
- Any machine without a password or passphrase is Protected by default
- Specify “NOPASSWORD” and “NOPHRASE” on ADDUSER or ALTUSER:

```
ALTUSER TCPIP10 NOPASSWORD NOPHRASE
```

- To remove the Protected attribute from a user, add a password or passphrase:

```
ALTUSER BWHUGEN PHRASE('Three measures of Gordons, one of vodka, half a measure of Kina Lillet')
```

- Protected users can still be revoked through REVOKE
- LOGONBY access still allowed

RAC SETROPTS LIST

(a small portion of the output)

PASSWORD PROCESSING OPTIONS:

PASSWORD CHANGE INTERVAL IS 186 DAYS.

MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT

NO PASSWORD HISTORY BEING MAINTAINED.

AFTER 5 CONSECUTIVE UNSUCCESSFUL PASSWORD
ATTEMPTS,

A USERID WILL BE REVOKED.

NO PASSWORD EXPIRATION WARNING MESSAGES WILL BE
ISSUED.

INSTALLATION PASSWORD SYNTAX RULES:

RULE 1 LENGTH(7:8) ALLLLLA*

RULE 2 LENGTH(8) ALLLLLLA

RULE 3 LENGTH(8) ALLLLLLA

LEGEND:

A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL
W-NOVOWEL *-ANYTHING

c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL
\$-NATIONAL

Example: PCI DSS and Shared Accounts

8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	8.5.8.a For a sample of system components, examine user ID lists to verify the following: <ul style="list-style-type: none">▪ Generic user IDs and accounts are disabled or removed▪ Shared user IDs for system administration activities and other critical functions do not exist▪ Shared and generic user IDs are not used to administer any system components
--	--

- Are you using **LOGONBY** in z/VM for privileged virtual machines?
- Is the password of that virtual machine set to **LBYONLY**?
- If RACF is installed on the system, has the **SURROGAT** class been activated?
- Are **successful** instances of the LOGON command **audited** for this virtual machine? Why or why not?

Example: PCI DSS and Shared Accounts

```
USER SSLDCSSM LBYONLY 32M 64M GE
  INCLUDE TCPCMSU
  LOGONBY TCPMAINT GSKADMIN BWHUGEN
  NAMESAVE TCPIP10
  OPTION QUICKDSP SVMSTAT
  LINK 6VMTCP20 0491 0491 RR
  LINK 6VMTCP20 0492 0492 RR
  LINK TCPMAINT 0591 0591 RR
  LINK TCPMAINT 0592 0592 RR
  LINK TCPMNT10 0198 0198 RR
  MDISK 0191 3390 523 5 12345A MR READ WRITE MULTI
```

Example: PCI DSS and “Least Privilege”

7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities

7.1.1 Confirm that access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.

- Do the virtual machines hosting your guest operating systems require more than z/VM Privilege Class G?
 - Do they require less?
 - Do they require a subset of a few of the defaults?
- Have your guest OS containers been assigned a non-default z/VM privilege class (a user-defined role, e.g. “L” for “Linux guests” or “V” for “VSE”)?
- **Note:** *user-defined privilege classes will not “auto-escalate” when upgrading your z/VM level.*

Example: PCI DSS and “Least Privilege”

Display commands available to your virtual machine:

```
QUERY COMMANDS
```

... or the privclass(es) applicable to a command you can currently issue:

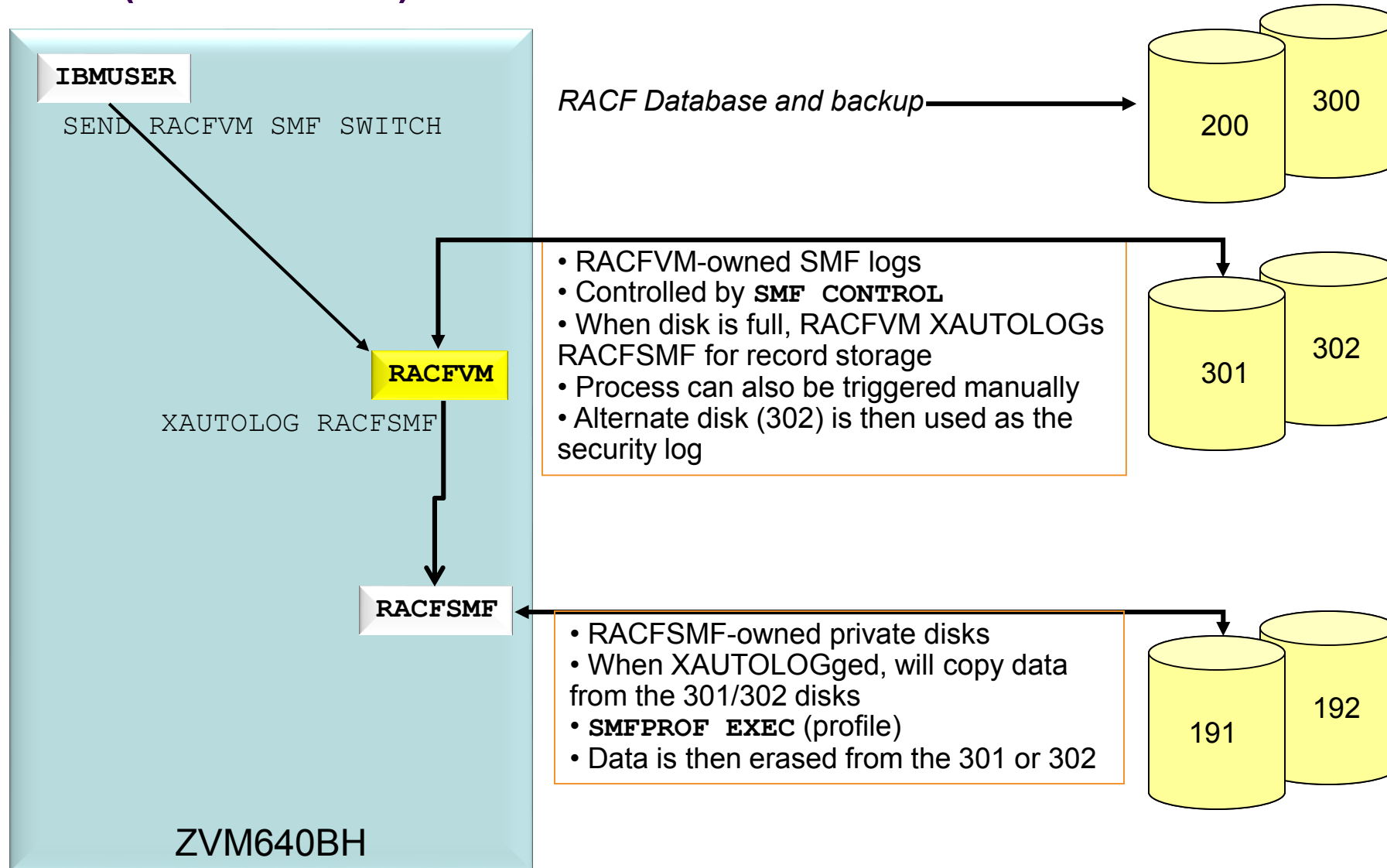
```
QUERY COMMAND <cmd>
```

Global modification – MODIFY CMD and MODIFY DIAGNOSE (Class A)
Also functions as an update to the System Configuration file.

Dynamically redefine a command into a different privilege class:

- MODIFY COMMAND SHUTDOWN PRIVCLASS S
- MODIFY COM XAUTOLOG IBMCLASS A PRIVCLASS X
- MODIFY CMD QUERY SUBCMD NAMES IBMCLASS G PRIVCLASS Z
- MODIFY COMMAND XAUTOLOG RESET
- MODIFY DIAG 94 PRIVCLASS V

Auditing RACF (An Overview)



Auditing RACF (A Little More)

- Settings to audit the actions of privileged users
 - **SAUDIT** Log all commands issued by SPECIAL users
 - **OPERAUDIT** Log any accesses made by OPERATIONS users
 - **CMDVIOL** Log all command violations (unauthorized usage)

- Settings to audit access attempts by class
 - Keywords **ALWAYS, NEVER, SUCCESSES, FAILURES**
 - Example: **SETROPTS LOGOPTIONS (ALWAYS (SURROGAT))**
 - Always log all attempts to use shared user ids

- Audit changes to profiles in a class
 - Example: **SETROPTS AUDIT (VMMDISK)**

- Can log audit records regularly, or when disk is full

RAC SETEVENT LIST (a subset)

PRE-LOGON COMMANDS

COMMAND	CONFIGURED IN
-----	-----
DIAL	YES
MESSAGE.ANY	YES
UNDIAL	YES

CONTROLLABLE VM EVENTS

VM EVENT	STATUS	VM EVENT	STATUS
-----	-----	-----	-----
COUPLE.G	CONTROL	FOR.C	CONTROL
FOR.G	CONTROL	LINK	CONTROL
STORE.C	CONTROL	TAG	CONTROL
TRANSFER.D	CONTROL	TRANSFER.G	CONTROL
TRSOURCE	CONTROL	DIAG088	CONTROL
DIAG0A0	CONTROL	DIAG0D4	CONTROL
DIAG0E4	CONTROL	DIAG280	CONTROL
DIAG290	CONTROL	APPCPWVL	CONTROL
MDISK	CONTROL	RSTDSEG	CONTROL

AUDITABLE VM EVENTS

VM EVENT	STATUS	VM EVENT	STATUS
-----	-----	-----	-----
ACNT	NO_AUDIT	ACTIVATE	NO_AUDIT
ADJUNCT	NO_AUDIT	ADSTOP	NO_AUDIT
ASSOCIATE	NO_AUDIT	ATTACH	NO_AUDIT
.

RACF Processing Options

- If RACF cannot record an event, the access should be denied and RACF should stop
 - SMF CONTROL file should say SEVER YES
 - Prevents unaudited events from occurring
 - May require SMF records to be processed more regularly

```
CURRENT 301 K PRIMARY 301 K SECONDARY 302 K 10000 VMSP CLOSE 001 SEVER YES 0 RACFSMF
```

- *Common Criteria evaluated configuration requirement*

RACF Processing Options

- RACFADU can be used to unload SMF records from the auditing disks
- Requires pertinent disk access and authorities – check the *Auditor's Guide* for details

ACCESS	SUCCESS	17:41:02	2013-02-06	VMSP	NO	NO	NO	CFCC2	SYS1	...
JOBINIT	RACINITI	17:41:02	2013-02-06	VMSP	NO	NO	NO	CFCC2	SYS1	...
JOBINIT	INVPSWD	21:03:56	2013-02-15	VMSP	YES	NO	NO	MAINT	SYS1	...
JOBINIT	INVPSWD	21:04:03	2013-02-15	VMSP	YES	NO	NO	MAINT	SYS1	...
ACCESS	SUCCESS	11:28:34	2013-03-26	VMSP	NO	NO	NO	BRIANH	SYS1	...

- Can also produce XML output to be fed into more friendly report writers
 - Or more high-end Business Analytics tools

zSecure Manager for RACF z/VM

- Provides audit & administrative usability improvements for RACF/VM and auditing for z/VM and Linux virtual machines on System z
- ISPF display-and-overtyping administration of RACF VM database
- Provides highly customizable reporting and analysis of audit records (SMF 8x (RACF), 83 (LDAP))
- Full support for auditing an administering RACF database
- Snapshot and analysis of z/VM security relevant setting (minidisks, real devices)
 - Analysis can be done both on z/VM and z/OS
- Snapshot and analysis of RACFVM security relevant settings (SYSSEC, GLBLDSK, CDT)
- Comparison of status (what changed)

```

Line 30 of 50
RACF CDT, SETROPTS class info and number of profiles
Command ==> _ Scroll==> CSR
10 Feb 2012 11:21
Complex System Classes Active Nonempty Profiles Audit concerns Priority
VM ZVM620 127 8 10 542 127 31
Pr Class Pos Grouping Members Protect Glbl Generic Profiles RC Oper RF
31 VMBATCH 15 Noaudit 124 4 OPER Ye

SYSSEC settings
SYSSEC Permit setting ALLOW SYSSEC Undefined setting DEFER
SYSSEC Warning setting DEFER SYSSEC Message setting
SYSSEC Failure setting FAIL

```



Measuring the Changes

Measuring the Changes



- All that time spent configuring the system ... what happens when a PTF comes out?
- What does that do to the Evaluated Configuration?
- What if it's a SEC/INT APAR?

Measuring the Changes

Certification

- z/VM's Common Criteria certification comes with "Flaw Remediation"
 - ALC_FLR.3: "Systemic Flaw Remediation"
 - You'll see this abbreviated as the + in "EAL 4+".
- Allows for the application of security-related patches onto the evaluated configuration without invalidating the certification
 - Makes no claims about PTFs **unrelated** to security

Compliance

- User-defined privileged classes prevent automatic escalation on the release boundary
- As we've noted, though, not all risks are equal.
 - How do we determine if this PTF is important?
 - **Are there any policy or industry requirements for annotating service, though?**

--why yes. Yes there are.

PCI DSS Requirements

6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.

Notes:

- *Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.*

"Is z/VM vulnerable to _____?"



"Is z/VM vulnerable to _____?"

- IBM Z Security policy **prohibits the general disclosure of vulnerability analyses (negative or positive)**. In part this is to prevent any inadvertent or malicious exploitation of vulnerabilities in System z environments which have not yet been updated to current levels of service.
- To stay current, your company can register with the IBM Z Security Portal in order to receive up to date lists regarding APAR/PTF information and CVSS scoring for SEC/INT service as it becomes available. In addition, Security Notices will be published through this website in order to address high-profile security issues, notifications and possible warnings.
- Access to the portal can be obtained through the following website:
http://www-03.ibm.com/systems/z/solutions/security_subintegrity.html

IBM Z Security Portal >> What Is It?

- Only available to IBM Z clients
- Clients must **register** to gain access
- Recommend clients **subscribe** for email notification
- Contains APAR/PTF numbers for all applicable exposures
 - Customers are considered exposed if they run affected product/component
 - No other details that could be used to potentially exploit are provided
- Industry standard scoring for risk assessment
- APAR/PTF fix information posted when fix is available
 - z/OS → SMP/E SECINT ++HOLDDATA and ++ASSIGN statements
 - z/VM → APAR/PTF/COMPID
- Security Notices for higher visibility vulnerabilities or issues
 - Including non-SMP/E products and general security communications

IBM Z Security Portal >> Security Notices

- **Security Notices** are text (bulletin-like) documents provided on the Security Portal to communicate [information for highly publicized vulnerabilities](#) that may generate many inquiries.
 - Introduced in 2014
 - Updated as investigation progresses and whenever new information is available
 - May include mitigations if pertinent

- Concerns with responding to vulnerability requests in a PMR:
 - investigation may still be in progress; may make responses **incomplete or inaccurate**
 - information may be **updated** several times through the investigation.
[Portal subscribers are notified each time there is an update.](#)
 - confirming an exposure with **no mitigation** puts all clients at risk
 - there are **many security fixes** identified on the Security Portal and reacting only to the highly publicized vulnerabilities is not a good/complete security process

Common Vulnerability Scoring System (CVSS v3)

- An open-standard metric for vulnerability measurement
 - <http://www.first.org/cvss/cvss-guide.html>
 - Not to be confused with a “threat rating system” or vulnerability catalogue

- z/VM provides a CVSS Score and Vector for Security-related z/VM APARs (“**ResourceLink**” information) for [subscribed customers](#)
 - http://www-03.ibm.com/systems/z/solutions/security_subintegrity.html
 - Vulnerabilities scored 0 to 10 based upon a range of criteria
 - Score plus vectors allow you to determine if this PTF requires more urgent attention

- IBM Internet Security Systems, similarly, includes CVSS base and temporal scores in its X-Force bulletins: <http://www.iss.net/threats/ThreatList.php>

Common Vulnerability Scoring System (CVSS v3)

- Comprised of three scores:
 - A **base metric** which measures complexity, levels of authentication, access vectors, and impacts to various aspects of security ([IBM provides](#))
 - A **temporal metric** which measures the exploitability of the threat and availability of a fix ([IBM provides](#))
 - An **environmental metric** which determines a vulnerability's impact to a specific configuration

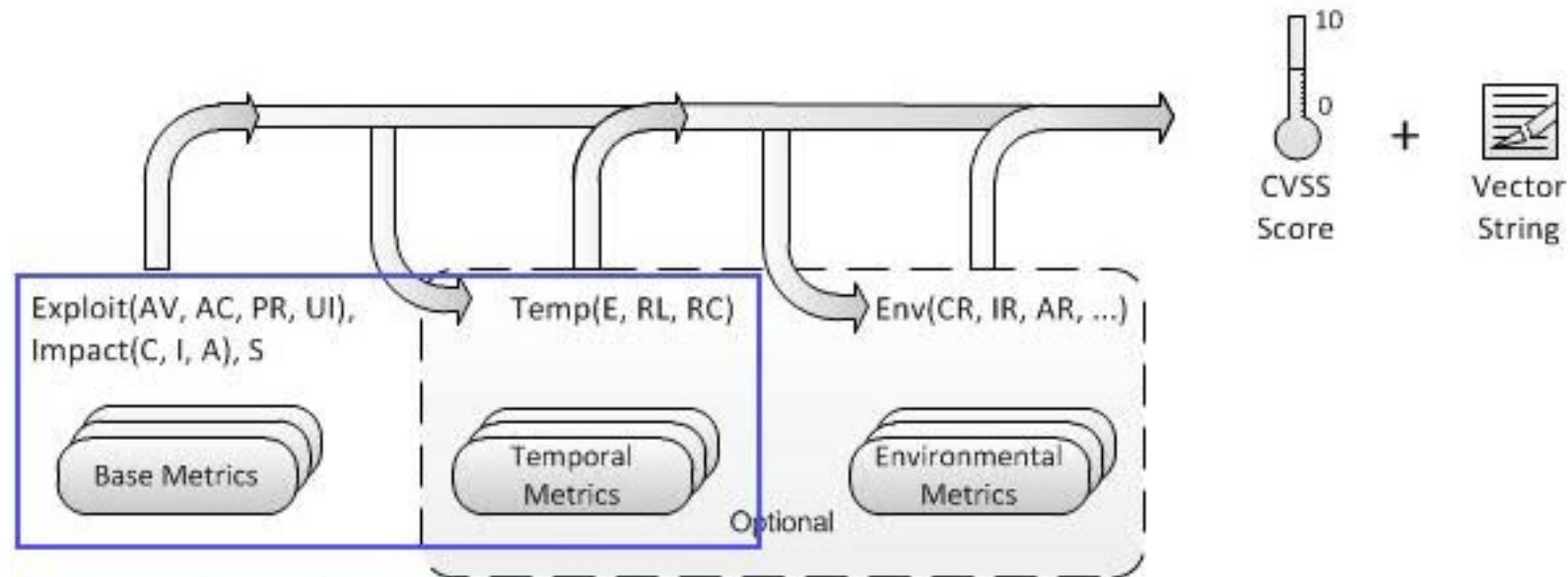



Figure 2: CVSS Metrics and Equations





IBM Z Security Portal >> Sample z/VM CVSS Data

* * IBM Confidential * *  Not Really ...

YrDay	COMPID	APAR	Rel	PTF	CVSS Base/Temporal/Vector
-----	-----	-----	-----	-----	-----
...					
00000	568411201	VM12345	R630	UM54321	4.3/3.7/ (AV:N/AC:M/Au:N/C:N/I:P/A:N/E:ND/RL:OF/RC:C)
00000	5735FAL00	PI23456	R630	UI65432	6.4/5.6/ (AV:N/AC:L/Au:N/C:P/I:N/A:P/E:ND/RL:OF/RC:C)
00000	5735FAL00	PI34567	R630	UI76543	7.5/6.5/ (AV:N/AC:L/Au:N/C:P/I:P/A:P/E:ND/RL:OF/RC:C)
00000	5735FAL00	PI45678	R630	UI87654	2.6/2.3/ (AV:N/AC:H/Au:N/C:P/I:N/A:N/E:ND/RL:OF/RC:C)
...					

 Dates removed

 APAR numbers changed

 PTF numbers changed

Example: a TLS “Man-in-the-Middle” Exploit

([Sample analysis](#). Does not represent a formal IBM analysis, or represent actual IBM service.)

Given the following vectors: (CVSS : 3 . 0 / AV : N / AC : L / PR : N / UI : N / S : C / C : H / I : L / A : N / RL : O / RC : C)

We can interpret them as follows:

- AV : N** -- Access is acquired through wide network, not local traffic
- AC : L** -- Access requirements are pretty low – just get in the middle. Complicated, but not esoteric.
- PR : N** -- No privileges on the system are required to execute the attack
- UI : R** -- The attacker must interact with the system to carry out the attack.
- S : C** -- The vulnerable component may lead to other components being impacted
- C : H** -- There is a high threat to information confidentiality. (Hacker may steal data.)
- I : P** -- There is a medium threat to data integrity. (Hacker may change or corrupt data depending on circumstance.)
- A : N** -- The hacker can’t actually bring down the system, though.
- E : ND** -- Exploitability isn’t defined.
- RL : O** -- There is an official fix available
- RC : C** -- Report Confidence is set to Confirmed

This flaw would be rated as a 8.9 out of 10.0. (Base Score 9.3; Temporal Score 8.9)

- *If the TLS/SSL Server is not defined on your system, Overall CVSS Score may be 0.*
- *This score is for z/VM only; **makes no statement about guest configuration!***

IBM Z Security Portal >> Finding Data (Once You're Registered)

The screenshot shows the IBM Z Security Portal in a Firefox browser. The address bar displays the URL: <https://www-304.ibm.com/servers/resourcelink/hom03010.nsf/pages/problemSolving?OpenDocument&login>. The page title is "Problem solving". The left sidebar contains a "Resource Link" menu with options: Site search, Planning, Education, Library, Fixes, Problem solving (highlighted), Services, Tools, Customer Initiated Upgrade, and Feedback. The main content area is divided into several sections: Hardware (Known defects/problems, Exception letters), Alerts (Machine alerts, Hiper alerts, Product support alerts, Red alerts, Security alerts), Report problems (Hardware problem reporting), Hardware service activities (Machine information), Other resources (System programmer portal, Linux for Mainframes), Report problems (Software problem reporting), Search technical databases (Troubleshooting, Tips and howto, Subscribe to APAR tracking), and Forums (z/OS and OS/390, z/VM and VM/ESA, VSE forums, Linux for zSeries). A red circle highlights the "Problem solving" link in the sidebar, and a red arrow points to the "Red alerts" link in the Alerts section. The footer contains links for Connect with us, Key topics, Information for, Shop & buy, About IBM, and Popular links. The Windows taskbar at the bottom shows the time as 12:33 PM.

IBM Z Security Portal >> Finding Data (Once You're Registered)

The screenshot displays the IBM Z Security Portal in a Firefox browser window. The address bar shows the URL: <https://www-304.ibm.com/servers/resourceLink/lib03020.nsf/pages/securityalerts/OpenDocument&start=1&count=500>. The page title is "Security alerts".

The left sidebar contains a "Resource Link" menu with the following items: Site search, Planning, Education, Library, Fixes, Problem solving (selected), Services, Tools, Customer Initiated Upgrade, and Feedback.

The main content area includes a "Subscribe" button circled in red. Below the header, there is a list of security alerts:

- z/OS Security/Integrity ASSIGNs Current ASSIGN File (last modified 20 Feb 2013)
- z/OS Security/Integrity CVSS Current CVSS file (last modified 20 Feb 2013)
- z/OS Security/Integrity Data Current HOLDDATA File (last modified 20 Feb 2013)
- z/VM Security/Integrity Data Current APAR Data (last modified 4 Feb 2013) → **z/VM Data**
- z/OS and z/VM SIA Cross Reference SIA Cross Reference (last modified 12 Feb 2013)
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in z/OS → **Security Notice**
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in DFSMS
- C-IBM-zSeries APAR [redacted] Security concern in USS
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in IOS
- C-IBM-zSeries APAR [redacted] System integrity concern in FRFS
- C-IBM-zSeries APAR [redacted] This issue pertains to users of Tivoli Service Desk (TSD).
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in DFSMS
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in DFSMS
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in z/OS - OS/390
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in DFSMS
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in DFSMS
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in RACF
- C-IBM-zSeries APAR [redacted] Possible system integrity issue in RACF

The bottom of the screen shows the Windows taskbar with various application icons and the system clock displaying 12:34 PM.



Measuring our Thesis

Summary

- **Security is a nebulous term because risks are, too**
 - Everyone will measure it a little differently ([units, units, units](#))
 - Security is a moving target--technologies and threats are changing
- **Learn company security policies and standards requirements**
 - The safest system in the world can be improperly configured
 - [Measure twice, cut once](#)
 - Be mindful of flaw remediation
- **Know how to prove your security**
 - [Security is meaningless without the data to back it up](#)
 - Not just for corporate audits, but in case The Worst Should Happen
 - [Knowing what you need to measure](#) – successes or failures – is important
- **We can only show you the door**
 - Prepare and Protect, Measure and Detect, Mitigate and Recover
 - Don't forget your hardware, network, guest access, clouds, mobile ...



For More Information ...

- **IBM Z Security:**

- <https://www-03.ibm.com/systems/z/solutions/enterprise-security.html>

- **z/VM Security resources:**

- <http://www.vm.ibm.com/security>

- **Securing Your Cloud: IBM z/VM Security** (SG24-7471), IBM RedBooks

- <http://www.redbooks.ibm.com/abstracts/sg248353.html?Open>

- **Security for Linux on System z** (SG24-7728), IBM RedBooks

- <http://www.redbooks.ibm.com/abstracts/sg247728.html?Open>

- **The IBM Z Security Portal FAQ:**

- https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ST&infotype=SA&appname=STGE_ZS_ZS_USEN&htmlfid=ZSQ03054USEN&attachment=ZSQ03054USEN.PDF

Contact Information:

[Brian W. Hugenbruch](#)

IBM Z Security for Virtualization and Cloud

[hwhugen at us dot ibm dot com](mailto:hwhugen@us.ibm.com)

 [@Bwhugen](#)

CISSP®



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

Dankon

Esperanto

Thank You

谢谢

Chinese

ありがとうございます

Japanese

Trugarez

Breton

Danke

German

Tak

Danish

Grazie

Italian

நன்றி

Tamil

děkuji

Czech

ขอบคุณ

Thai

go raibh maith agat

Gaelic