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

zSI: z/VM Security Investigation

or, A Discussion on Measuring z/VM Security

#WAVV #zVM #IBMSecurity

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.

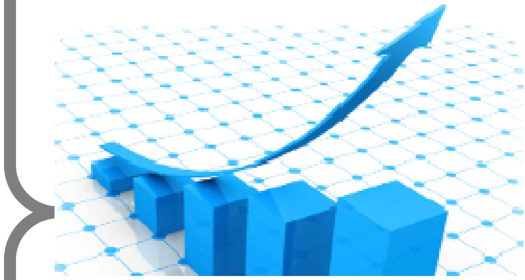
It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming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

Objective

The intent of this presentation is to help a system administrator determine what constitutes the scope of “virtualization security” – and, by extension, how to determine if it’s working.

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



You received your magnifying glasses at conference registration, right?

AES	Advanced Encryption Standard
ARL	Authority Revocation List
CA	Certification Authority
CBC	Cipher Block Chaining
CCA	IBM Common Cryptographic Architecture
CCF	Cryptographic Coprocessor Facility
CDSA	Common Data Security Architecture
CEX2/3A	Crypto Express 2/3 Accelerator Mode
CEX2/3C	Crypto Express 2/3 Coprocessor Mode
CFB	Cipher Feedback
CKDS	Cryptographic Key Data Set
CRL	Certificate Revocation List
CRT	Chinese Remainder Theorem
CVC	Card Verification Code
CVV	Value
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Standard
ECB	Electronic Code Book
FIPS	Federal Information Processing Standard
GSS	Generalized Security Services
ICSF	Integrated Cryptographic Service Facility
IETF	Internet Engineering Task Force
IPKI	Internet Public Key Infrastructure
KGUP	Key Generation Utility Program
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MDC	Message Detection Code
MD5	Message Digest 5
OAEP	Optimal Asymmetric Encryption Padding
OCSF	OS/390 Open Cryptographic Services Facility
OCSP	Online Certificate Status Protocol
PCICA	PCI Cryptographic Accelerator
PCICC	PCI Cryptographic Coprocessor
PCIXCC	PCIX Cryptographic Coprocessor
PKA	Public Key Architecture
PKCS	Cryptographic Standards
PKDS	Public Key Data Set
PKI	Infrastructure
RA	Registration Authority
RACF	Resource Access Control Facility
RSA	Rivest-Shamir-Adleman
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SLE	Session Level Encryption
SSL	Secure Sockets Layer
TKE	Trusted Key Entry
TLS	Transport Layer Security
VPN	Virtual Private Network

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

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

Answer unclear; please try again.

- “Well, that’s just RACF, isn’t it?”

Information security is a set of mechanisms

through which

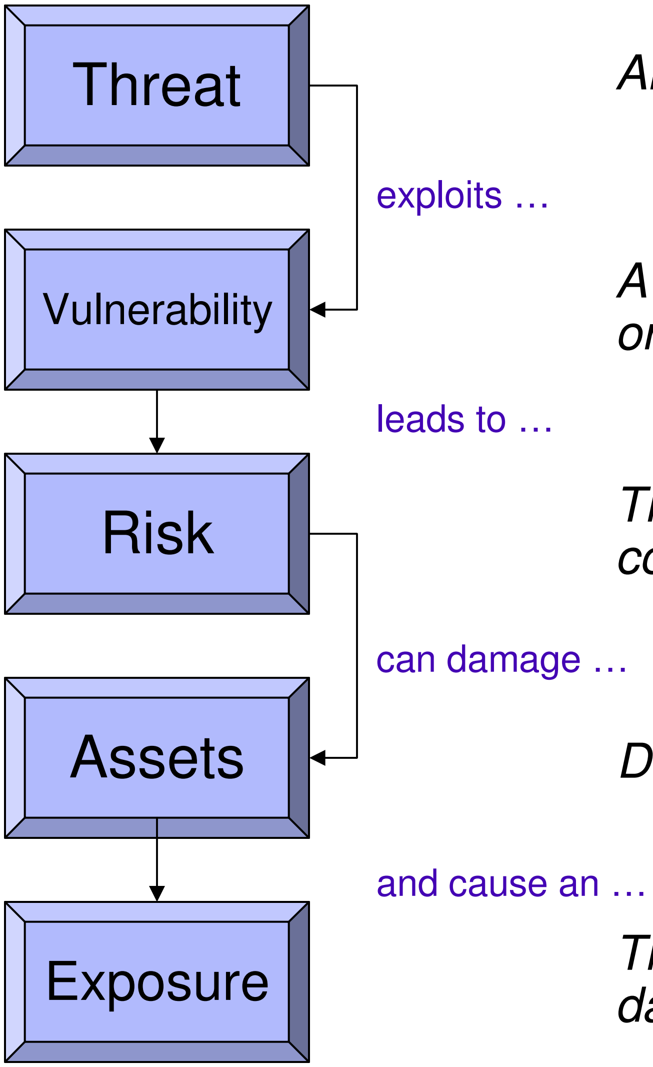
the **availability, integrity, and confidentiality** of

assets (e.g., resources, services, and data)

are preserved and protected

against potential **threats**.

Vulnerabilities, Threats, and Risk



Any potential danger to information or systems.

A weakness in an information system (software, hardware, or procedural).

The likelihood of someone exploiting a vulnerability, with corresponding impacts to business.

Data, services, systems …

The result of a vulnerability being exploited – e.g., damaged assets, disrupted business, legal action.

How big of a risk is it?

- Not every risk leads to an exposure
- Not all threats are created equal
- Not all assets carry the same value

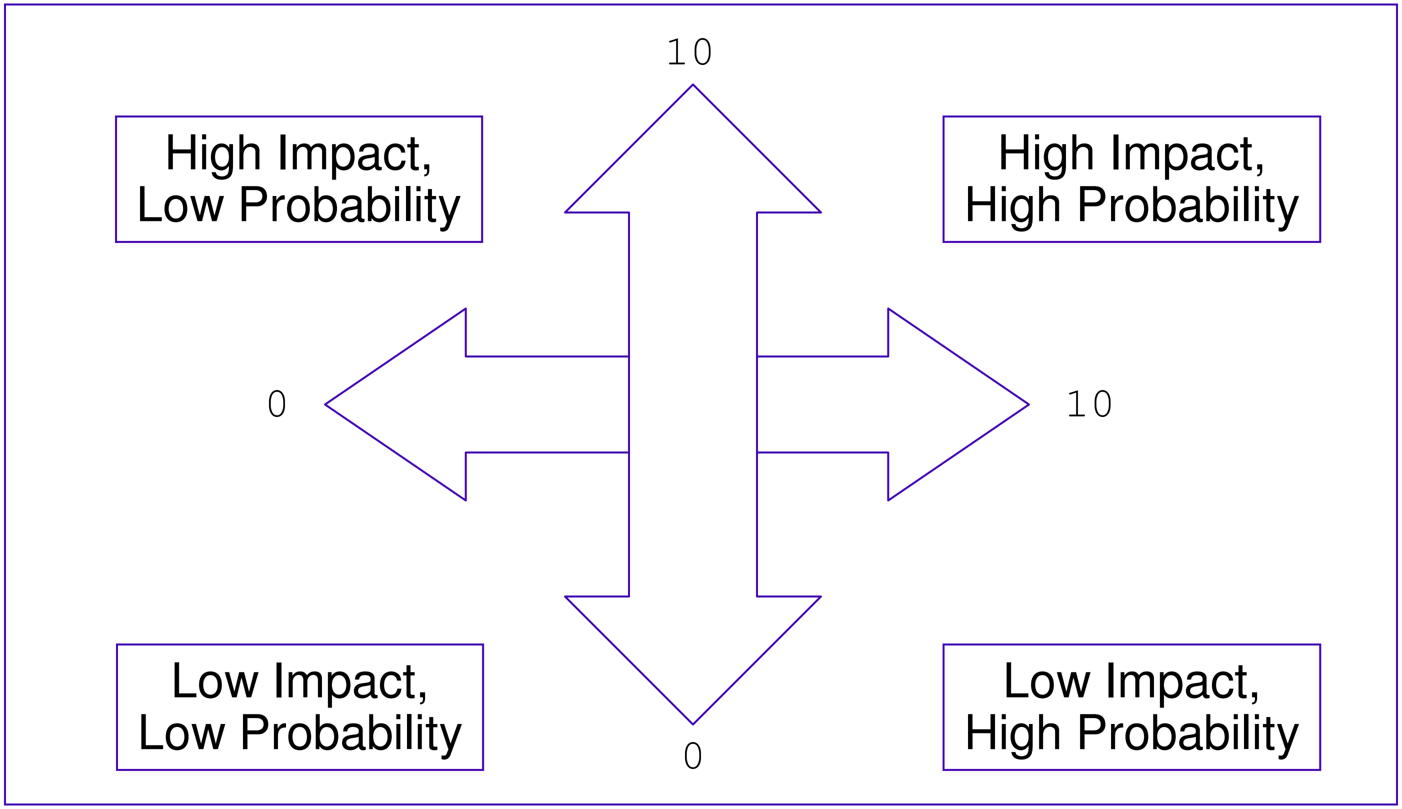
- **Quanitative – the numerical approach**
  Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO) == ALE

Asset	**Threat**	**SLE**	**ARO**	**ALE**
Facility	Flood	250K (USD)	0.001	250 (USD)
Customer CC	Stolen	300K (USD)	5	1.5M (USD)

  - **Pros**: assigns hard currency to the risks, enables cost/benefit analysis, automatable
  - **Cons**: Laborious, time-intensive, no standards available, may ignore SMEs

How big of a risk is it?

- **Qualitative Approach**

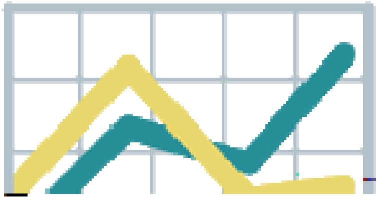

10
High Impact, Low Probability
High Impact, High Probability
0
10
Low Impact, Low Probability
0
Low Impact, High Probability

  - **Pros**: less math, pulls in the perspective of subject-matter experts
  - **Cons**: Subjective analysis, difficult to track and account, standards not available

Key Performance Indicators might be useful …

An approach of measuring security using quantitative metrics.

- *Weighted Risk Trend* (WRT): a risk score measured over time.
- *Rate of Defect Recurrence* (RDR): rate at which closed defects reappear.
- *Specific Coverage Metric* (SCM): the percentage of tested components, relative to all components under review.
- *Security-to-Quality Defect Ratio* (SQR): the number of security-specific defects uncovered during testing, relative to all quality defects uncovered.

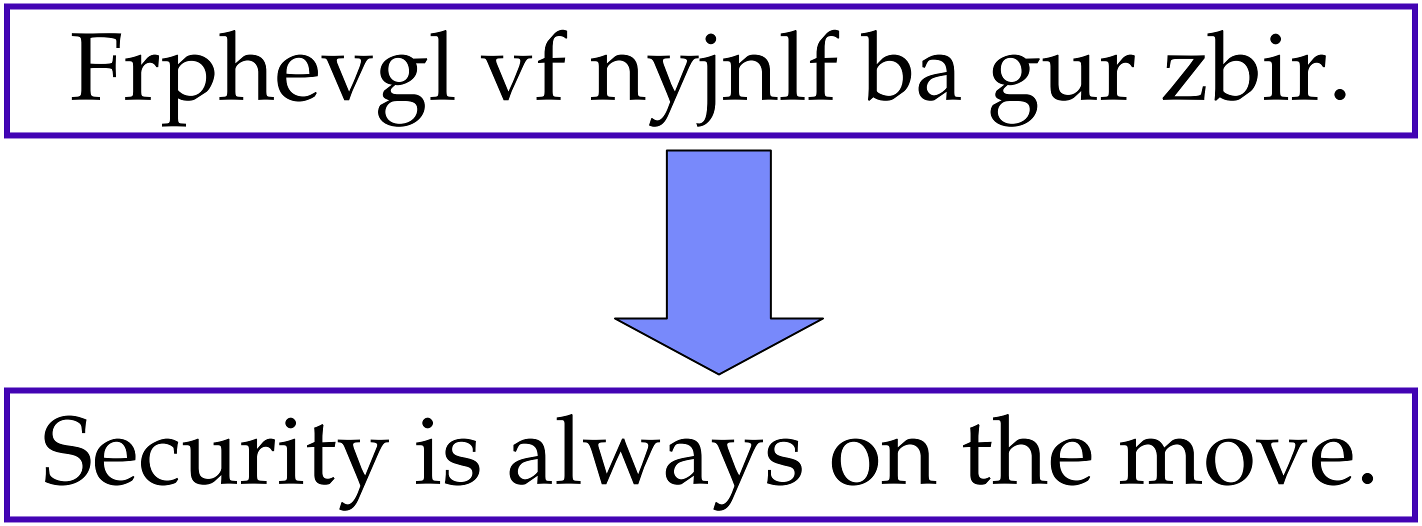


… but numbers are weird.

- 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?

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.

Certifications

Or, Measuring the Base Product

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

“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

• *Can be an Enumerated functional specification (e*.g., PR/SM evaluations)

It's tempting to say one Profile is better than another. It's instead a question of best fit for purpose – know your units.

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

• **EAL 1**: back-of-envelope sketch
• **EAL 2** through **6**: More and more comprehensive design, test, service; more functional requirements.
• **EAL 7**: Mathematical proof with exhaustive tests

It's tempting to focus on the EAL number as a "level of security." It's instead the extent of proof – but it is meaningless without the security target.

z/VM Security Certification Discussion

- The Common Criteria evaluated configuration of z/VM 6.1 includes:
  - z/VM Control Program, TCPIP, Telnet, RACFVM (included in previous evaluations)
  - z/VM SSL Server *new*

- Evaluated to the **Operating System Protection Profile** (OSPP)
  - Extensions for Labeled Security (-LS) and Virtualization (-VIRT)
  - Replaces the expired CAPP and LSPP profiles.

- **A particular configuration** of these parts is required
  - See the *z/VM 6.1 Secure Configuration Guide*
  - Lists associated service to apply

- Security-related service can be applied without invalidating the configuration
  - EAL4 "+" – "Flaw Remediation"

z/VM Security Certification Discussion

- OSPP-LS with EAL 4+ for the evaluated configuration has looked at the following:
  - Development processes, service processes, site security
  - Documentation and internal testing of
    - CPACF, System SSL for z/VM, RACF
    - Information flow control, Role-based, Discretionary, and Mandatory Access controls
    - Auditing; Separation of Auditing from Security Administration
    - Protection of Security Functions
  - Password policy control, revoking of userids, object reuse, terminal locking …….

FAU_GEN.1
FAU_GEN.2
FAU_SAR.1
FAU_SAR.2
FAU_SAR.3
FAU_STG.1
FAU_SEL.1
FAU_SEL.3
FAU_SEL.4
FCS_CKM.1
FCS_CKM.2

FCS_CKM.4
FCS_COP.1
FCS_RNG.1
FDP_ACC.1
FDP_ACC.2
FDP_ACF.1
FDP_ETC.2
FDP_IFC.2
FDP_IFF.1
FDP_ITC.2
FIA_AFL.1

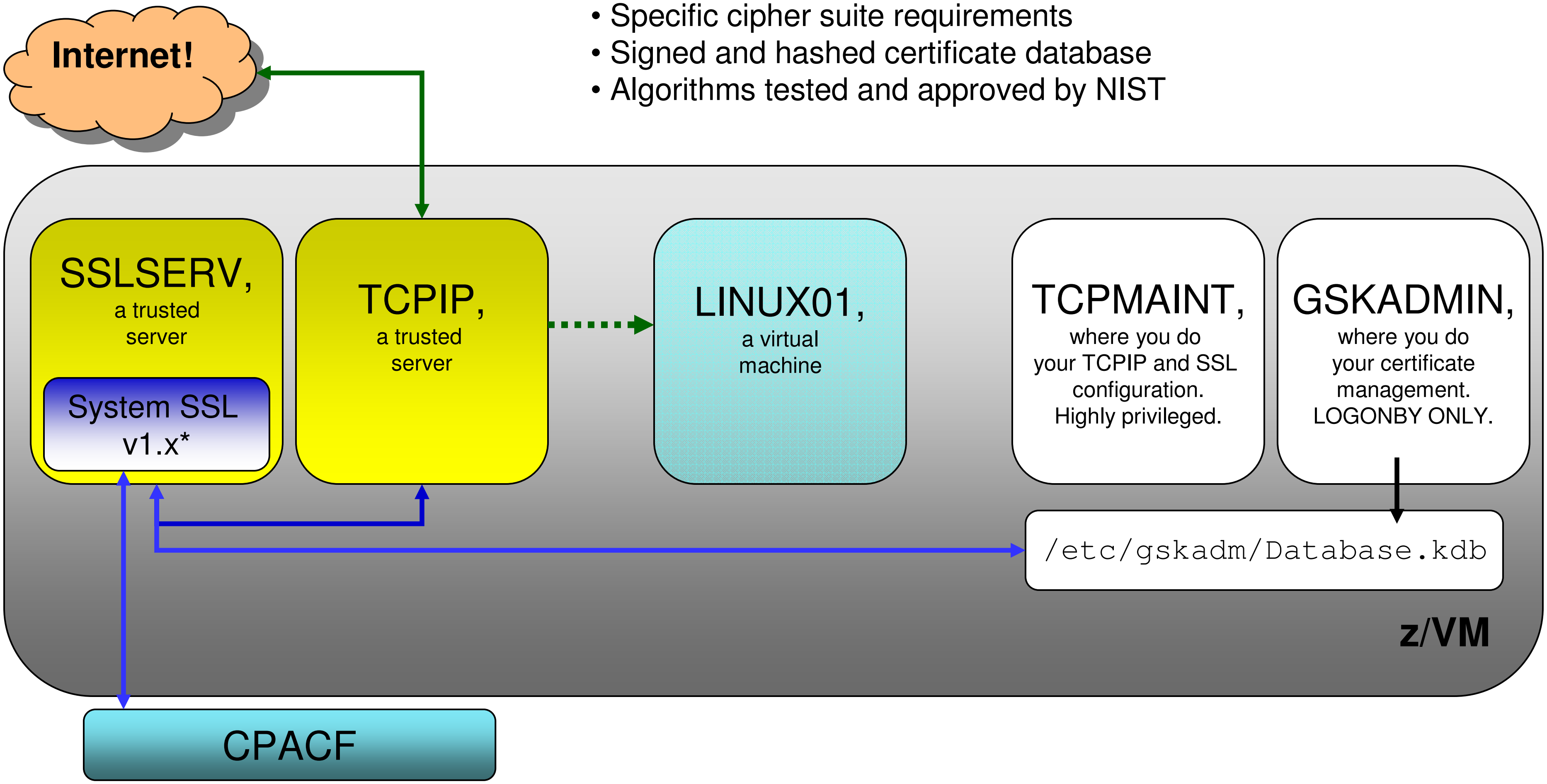
FIA_ATD.1
FIA_SOS.1
FIA_UAU.1
FIA_UAU.5
FIA_UAU.7
FIA_UID.1
FIA_UID.2
FIA_USB.1
FIA_USB.2
FMT_MSA.1

FMT_MSA.3
FMT_MTD.1
FMT_REV.1
FMT_SMF.1
FMT_SMR.1
FPT_STM.1
FTP_ITC.1
FTA_SSL.1
FTA_SSL.2
FDP_RIP.2
FDP_RIP.3

Federal Information Protection Standard (FIPS) 140-2

… in the z/VM SSL Server:

- Specific cipher suite requirements
- Signed and hashed certificate database
- Algorithms tested and approved by NIST



Internet!
SSLSERV, a trusted server
System SSL v1.x*
TCPIP, a trusted server
LINUX01, a virtual machine
TCPMAINT, where you do your TCPIP and SSL configuration. Highly privileged.
GSKADMIN, where you do your certificate management. LOGONBY ONLY.
/etc/gskadm/Database.kdb
z/VM
CPACF

FIPS 140-2 Analysis involves …

Compliance

Or, Measuring the Configuration

- But certificatio nn ng of t

- It declares “the toolb full.” D ow ho se hos
  are you building?

- 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? Something that hasn’t been invented yet?

- 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

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

A **regulation**,

The security **consideration** involved,

The z/VM **applicability**,

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

Example: PCI DSS and Default Passwords

[redacted]

- 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 in z/VM 6.2 for service virtual machines?

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

[redacted]

- 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 S10DCSSM LBYONLY 32M 64M GE
   INCLUDE TCPCMSU
   LOGONBY TCPMAINT GSKADMIN TCPMNT10 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”

[redacted]

- 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>
```

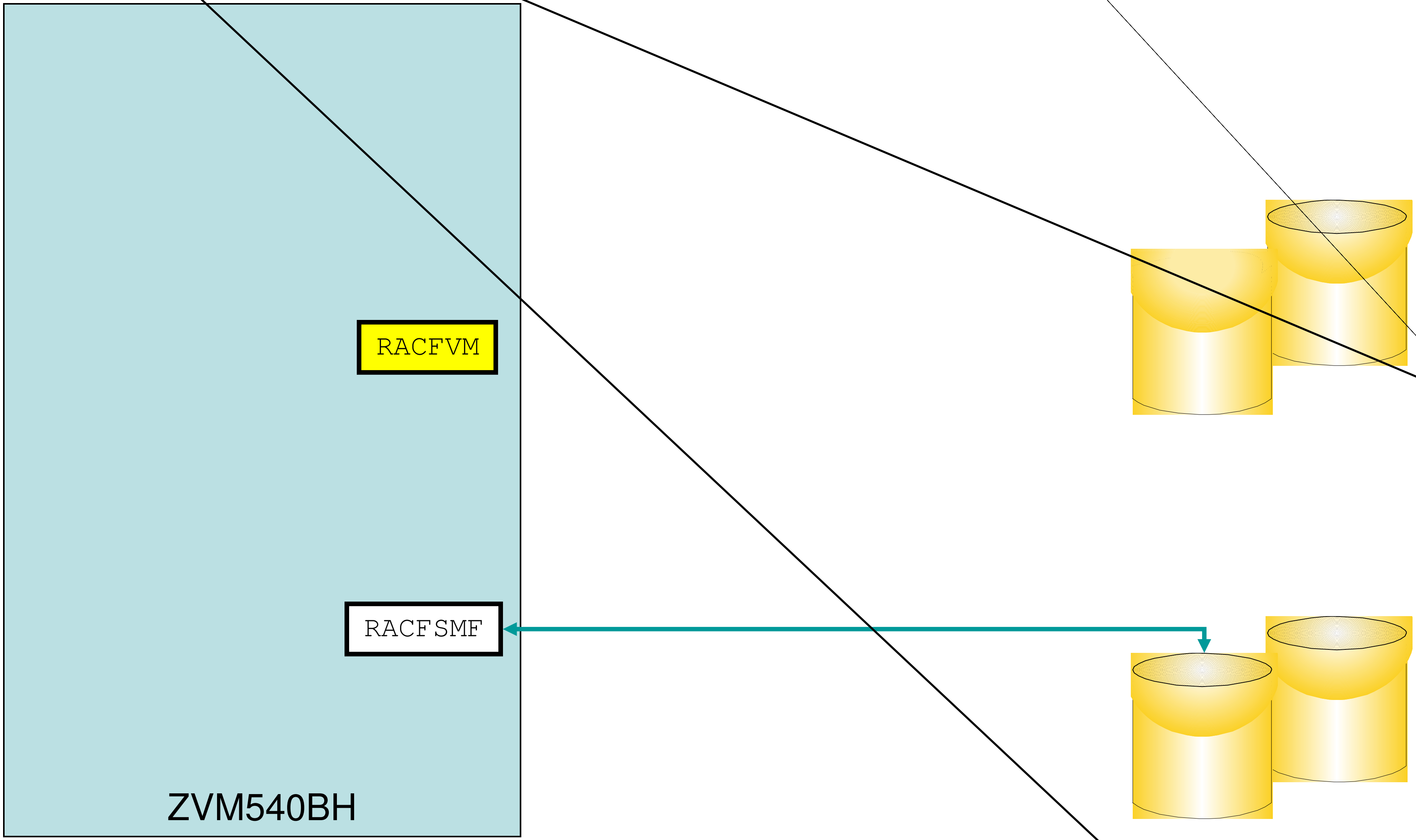
Global modification – `MODIFY CMD` and `MODIFY DIAGNOSE` (Class A)

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 RACFVM (The Basics)



#WAVV #zVM #IBMSecurity

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 small portion of the output)

```
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 ….

Changes

Or, Measuring the Fixes

Measuring the Fixes

- 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 Fixes

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

--why yes. Yes there are.

Common Vulnerability Scoring System (CVSS v2)

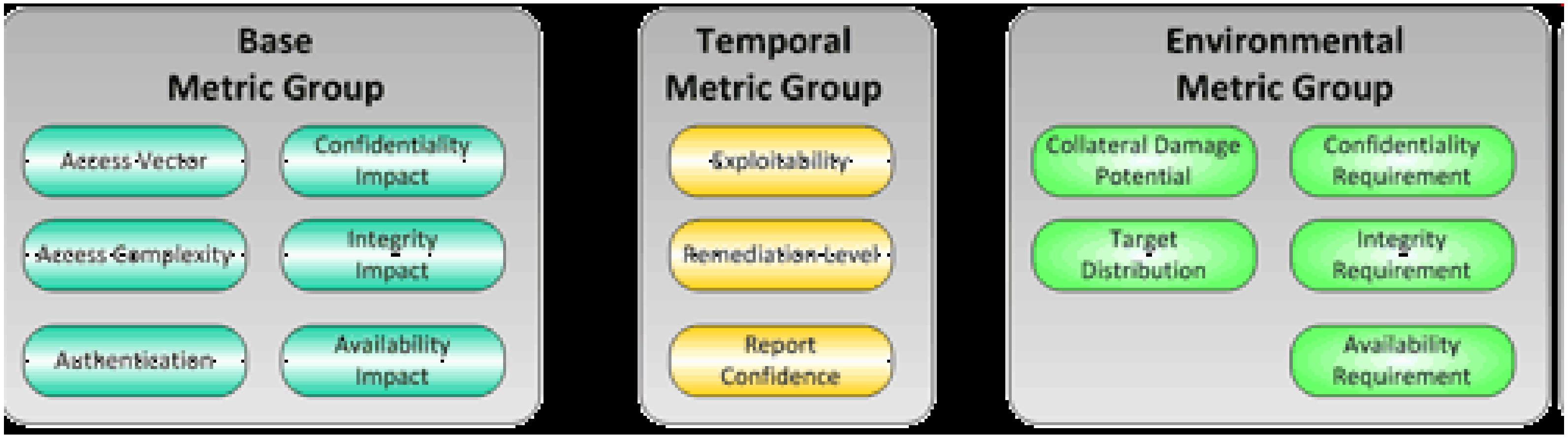
- An open-standard metric for vulnerability measurement
  - http://www.first.org/cvss/cvss-guide.html
  - Not to be confused with a “threat rating system” or vulnerability catalogue

- z/VM provides a CVSS Score and Vector for Security-related z/VM APARs (“ResourceLink” information)

- 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 v2)

- Comprised of three scores:
  - A **base metric** which measures complexity, levels of authentication, access vectors, and impacts to various aspects of security;
  - A **temporal metric** which measures the exploitability of the threat and availability of a fix; and
  - An **environmental metric** which determines a vulnerability's impact to a specific configuration, including the potential for collateral damage and percent of a business that might be under threat.



Example: an SSL “Man-in-the-Middle” Exploit

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

Given the following vectors: (`AV:N/AC:M/Au:N/C:P/I:P/A:N/E:ND/RL:O/RC:C`)

Where:

`AV:N   --` access through wide network, not local traffic
`AC:M   --` Access requirements are medium. Complicated, but not esoteric.
`Au:N   --` No system authentication is required.
`C: P   --` There is a partial threat to information confidentiality. (Hacker may steal data.)
`I: P   --` There is a partial threat to data integrity. (Hacker may change or corrupt data.)
`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 exploit is rated as a 5.0 out of 10.0. (Base Score 5.8; Temporal Score 5.0.)

If SSL is not defined on your system, Overall CVSS Score may be 0.

Example: Susceptibility to a Denial-of-Service packet storm

(Sample analysis. Does not constitute a formal IBM analysis, or represent actual IBM service.)

Given the following vectors: (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:ND/RL:O/RC:C)

Where:

AV: N -- access through wide network, not local traffic
AC: L -- Access requirements are low. This is a script kiddie running software.
Au: N -- No system authentication is required.
C: N -- There is no threat to information.
I: N -- There is no threat to data or system integrity.
A: C -- The hacker may knock systems offline or prevent services from being accesed.
E: ND -- Exploitability isn’t defined.
RL: O -- There is an official fix available
RC: C -- Report Confidence is set to Confirmed

This exploit is rated as a 6.8 out of 10.0. (Base Score 7.8; Temporal Score 6.0.)

If your business requires 24/7 availability, the Overall CVSS Score may be 8.7.

Conclusion

Or, Measuring Our Thesis

For More Information …

- **System z Security:** http://www.ibm.com/systems/z/advantages/security/
- **z/VM Security resources:** http://www.vm.ibm.com/security
- ***z/VM Security*** (SG24-7471), IBM RedBooks
- ***Security for Linux on System z*** (SG24-7728), IBM RedBooks
- ***z/VM Secure Configuration Guide***: http://publibz.boulder.ibm.com/epubs/pdf/hcss0b30.pdf

Contact Information:

Brian W. Hugenbruch, CISSP
z/VM Security Design and Development
bwhugen at us dot ibm dot com
+1 607.429.3660
Twitter: @Bwhugen

[redacted]

#zVMforTheWin

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

ขอบคุณ
Thai

děkuji
Czech

go raibh maith agat
Gaelic