

The Fundamentals of z/VM Security and Cyber Resiliency

Or: z/VM Security—ELI5

Brian W. Hugenbruch, CISSP
bwhugen@us.ibm.com  @Bwhugen

Agenda

Who am I, and what am I doing here?

“How do I secure z/VM?”

In just twelve easy steps...

Suggested Practices

Time for questions (or a nap)

An
MVMUA
Original
Presentation

Who am I?

- “Sir Brian, Wielder of the Security Hammer”
- 21 years as a z/VM Developer
 - CP, TCPIP, TLS, RACF coding
 - CP, Virtual Networking, RACF functional verification
- 11 years as the z/VM Security Champion
 - Roadmap for z/VM security development (not just for RACF)
 - Four Common Criteria certifications completed
 - Four FIPS 140-2 evaluations completed
 - Sponsor user discussions and research around security, ease of use, ...
- 1 year as LinuxONE Resiliency Lead
 - Because I needed more to do
 - Yes, I’m one of those people who count 9’s
- Most common question I receive?



“How do I secure z/VM?”

- Fantastic question!

- Brian answers this question with another question:
 - “What are you doing with it?”

- Is this system...
 - A production LPAR hosting traditional Linux guests, with three system programmers?
 - A development LPAR with 491 human users, each with their own CMS guest?
 - A test LPAR for testing Cloud Service scalability?

Recommendations For Virtual Environments

(An example list from the PCI DSS v2 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. Where do we start?

(Answer: “The beginning.”)

1. Know your rules

It might sound obvious, but especially in a large enterprise, **the number of rules** to which you must adhere is non-trivial

- *Just because no one's told you about the rules does not mean they're not there.*

In an ideal world, you start with the rules and then build the system

When inheriting architecture, this isn't always possible

Step 1: know your system

Step 2: know the technology

Step 3: know your requirements

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

z/VM Security Certifications

V7.2 Statements of Direction -- April 14, 2020

z/VM Level	Common Criteria	
z/VM V7.2 SoD	BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+ -- Completed!	NIAP VPP with Server Virt. Extended Package
z/VM 7.1	<i>Not evaluated ("designed to conform to standards")</i>	
z/VM 6.4	OSPP with Labeled Security and Virtualization at EAL 4+ -- COMPLETED! http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/in-corso-di-valutazione	
z/VM 6.3 (Out of Service)	OSPP with Labeled Security and Virtualization at EAL 4+ -- COMPLETED! • was valid through March 2020	



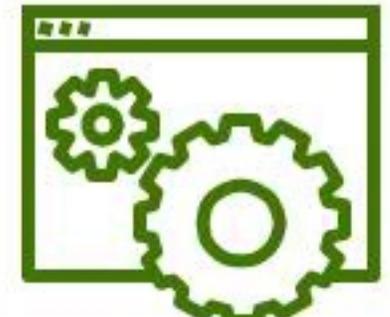
z/VM Level	FIPS 140-2
z/VM V7.2	FIPS 140-2 L1 for z/VM System SSL and ICSFLIB – Completed!
z/VM 7.1	<i>Not evaluated ("designed to conform to standards")</i>
z/VM 6.4	FIPS 140-2 L1 -- COMPLETED! https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3374
z/VM 6.3 (Out of service)	FIPS 140-2 L1 -- COMPLETED!



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

... but certifications aren't "enough."

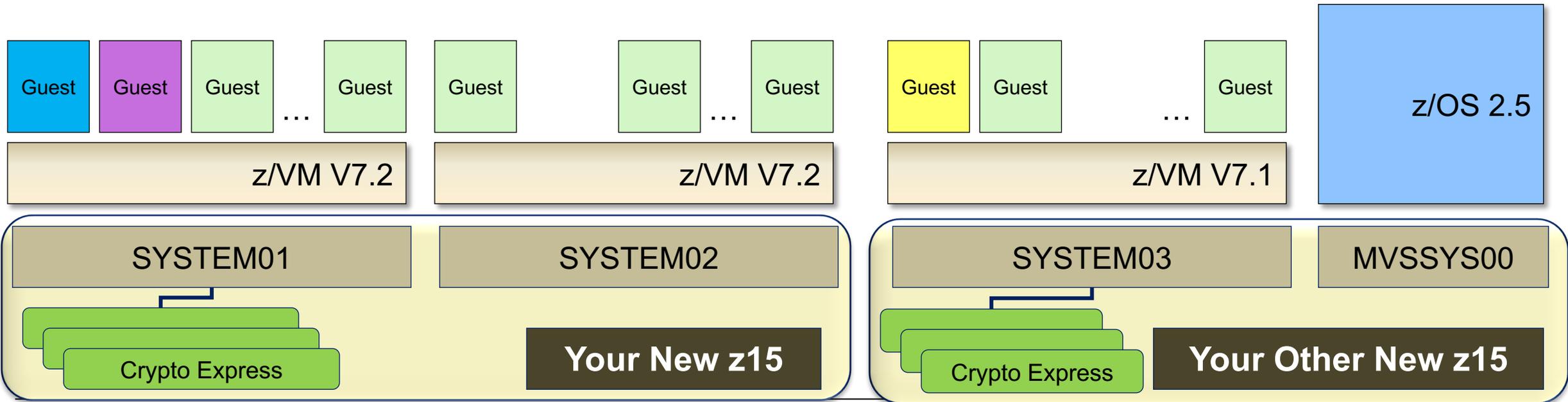
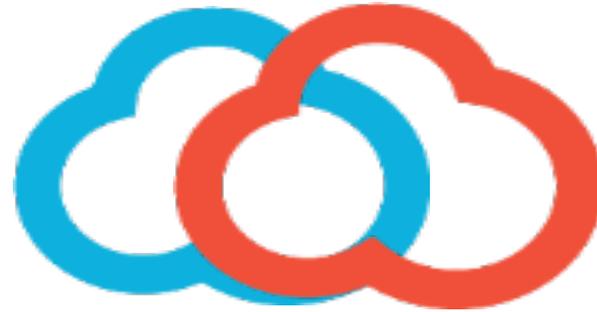
- z/VM Development does its best to give you the capabilities you need to defend your installation
- z/VM Development does not know every regulation or law to which you need to adhere
- All certifications for information security will require a particular configuration.
 - This includes z/VM Common Criteria 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."



2. Knowing your data

- Rules change depending upon the classification of the data in use in your z/VM partition
 - Prod is more restrictive than test
 - Prod has live client data
 - **Test better not have live client data!**
 - Prod has different resiliency and up-time requirements than test...
 - Security is no different
 - Dev is a strange, strange place
 - Not necessarily client data, but ‘secret sauce’ work which may have distinct requirements
- Pro Tip: the PCI DSS v3 asks you to draw diagrams of where Cardholder Information (CHI) flows
 - Reminder: that’s not cut-and-dried in a virtualized environment...

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



3. Change your defaults

- Shrink-wrap attacks
- IBM z/VM Development does not change its defaults as fast as this speaker would like
- Go through the System Configuration file, User Directory, and feature defaults to toggle things like:
 - Default privilege classes for basic workload
 - OPERATOR Privclass and ALTERNATE_OPERATOR
 - TDISK Clearing (**enabled by default in z/VM V7.2**)
 - **Default passwords in the z/VM user directory (also applies to minidisks)**
 - Virtual machine existence
 - Not using SMAPI? NOLOG it
- A useful evaluation both for new installs and existing infrastructure – challenge your own assumptions

4. Only humans need passwords

- By default, a lot of virtual machines have their own distinct passwords in the CP User Directory
 - They shouldn't. They're not on the payroll; they can't be fired if there's a breach.
 - And you're certainly not sharing passwords for OPERATOR amongst administrators!
 - Passwords should be socially distanced
 - And not just by putting the Post-It Note six feet away

- IBM is making progress on the default user directory, but that doesn't impact existing systems
 - And there's more work to do here...
 - Which means that you should investigate your own systems
 - Convert anything that isn't already LBYONLY or AUTOONLY
 - Give passwords only to human users
 - And revoke the humans when pertinent

5. Least Privilege

- Class G is defined for CMS General Users created in 1984
 - There are 60 Class G commands today, not including QUERY and SET
 - Linux requires ~15 of them to IPL

- Don't give out an entire privilege class for one command
 - Class C contains the FOR and SEND commands.
 - But it also contains STORE HOST
 - See also: COMMAND statement in the User Directory

- IBM z/VM Development does not change its defaults as fast as this speaker would like

- Any time IBM creates a new CP command, they go into the existing privilege classes

- Having user-defined content allows you to restrict guest access (either for Linux servers or human administrators) in accordance with policy, e.g.
 - L for Linux guests
 - P for Programmers
 - S exclusively for the SHUTDOWN command

5. Least Privilege

So what options are available?

1. Local modification – SET PRIVCLASS (Class ANY and Class C)

- Remove class authority from inside a virtual machine.
 - SET PRIVCLASS * -AC
- But be careful; the Class C version can exceed directory-granted privilege!

2. Global modification – MODIFY CMD and MODIFY DIAGNOSE (Class A)

- Dynamically redefine a command into a different privilege class.
 - MODIFY COMMAND SHUTDOWN PRIVCLASS S
 - MODIFY COM XAUTOLOG IBMCLASS A PRIVCLASS OUX
 - MODIFY CMD QUERY SUBCMD NAMES IBMCLASS G PRIVCLASS Z
 - MODIFY COMMAND XAUTOLOG RESET
 - MODIFY DIAG 94 PRIVCLASS V

6. Enable TLS for z/VM

- z/VM does not enable TLS by default. (It should, but it doesn't.)
- If your Rules (**see #1**) mandate that administrative access to systems must be encrypted, then TLS must be enabled.
 - The hypervisor is a point of entry
 - Linux has its own TCP/IP stack and encryption, but that doesn't help your CP LOGON screen
- If they don't... it's still a good idea, honestly
 - Data transferred in the clear can be observed (**see #2**)
 - Humans reuse passwords
 - And new technology (**Direct-to-host Service Transfer**) requires it
- TLS for z/VM has been FIPS 140-2 validated (through z/VM V7.2)
 - Cryptographic policy is configurable based on your needs
 - We're working on making certificate management easier (see: CERTMGR, available in 12/2021)
- See also: [The Junior Woodchuck's Guide to Using TLS on z/VM](#)
 - Presented at MVMUA in April 2021
 - <https://www.mvmua.org/21041210.pdf> (there's also a video)

7. Install and Enable an External Security Manager

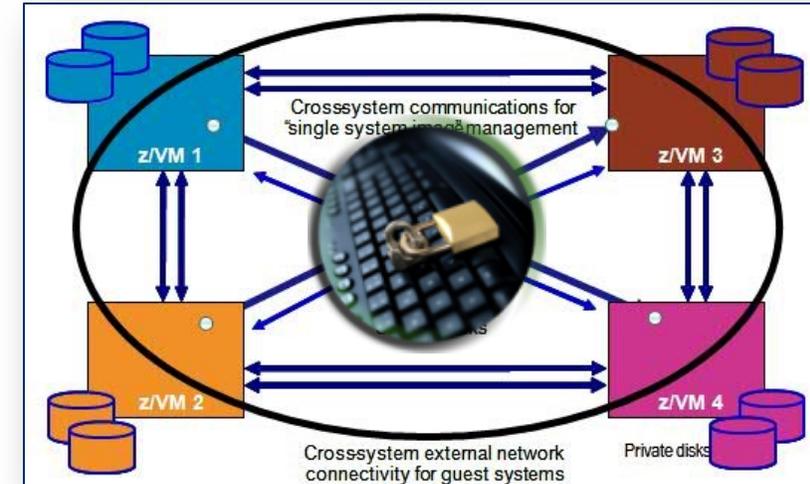
- Yes, really.
 - Yes, “if needed.”
 - But back that up with your rules. (**See #1**)

- I’m going to say ‘RACF’ a lot over the next few slides.
 - But, honestly, if you have one of the other ESM’s, I’m cool with it.
 - All I care about is that you’re computing safely.

- If you have **no ESM**, though, your system cannot meet the industry standards and regulations through which all modern IT is built.
 - Where by “modern” I mean 2003.

7. Install and Enable an External Security Manager

- 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+)*



7. Install and Enable an External Security Manager

- “But we only have one administrator!”
 - Did the Rules (**see #1**) have an “[Except for Bill, we know he’s cool](#)” clause?
 - If Bill’s bribed in dollars or dogecoins, what tracks the damage he might do to the system?

- “Do you have RACF installed?” “...yes?”

- “We already have a control policy” (Three Stooges story)
 - Consider auditing
 - Consider collusion
 - Consider your choices again (and **see #1**)

- “It’s too complicated!”
 - There are ways IBM can help with that (see: Lab-Based Services)
 - There are ways programs can help with that (see: zSecure for RACFVM or similar)
 - There are ways **you can help us** with that (see: VM Council)
 - *We can’t fix the problems we’re not seeing*

8. Deploy Multifactor Authentication

- **If needed.**
 - Again, **see #1**
 - This is where a closer understanding of the Rules will help.

- That said, passwords are understood to be a technology that can be compromised
 - Humans don't generate strong ones willingly
 - Humans will rotate them or reuse them

- Use of a second authentication factor (“something you have” or “something you are”) can strengthen your system against compromise of a single password

- On z/VM, this requires the IBM Z Multi-factor Authentication product.... as well as an ESM.
 - *Honestly, we figured if you didn't have an ESM, you didn't care about security*
 - *So, no, we're not enabling MFA for an ESM-less system.*

IBM Z Multi-factor Authentication

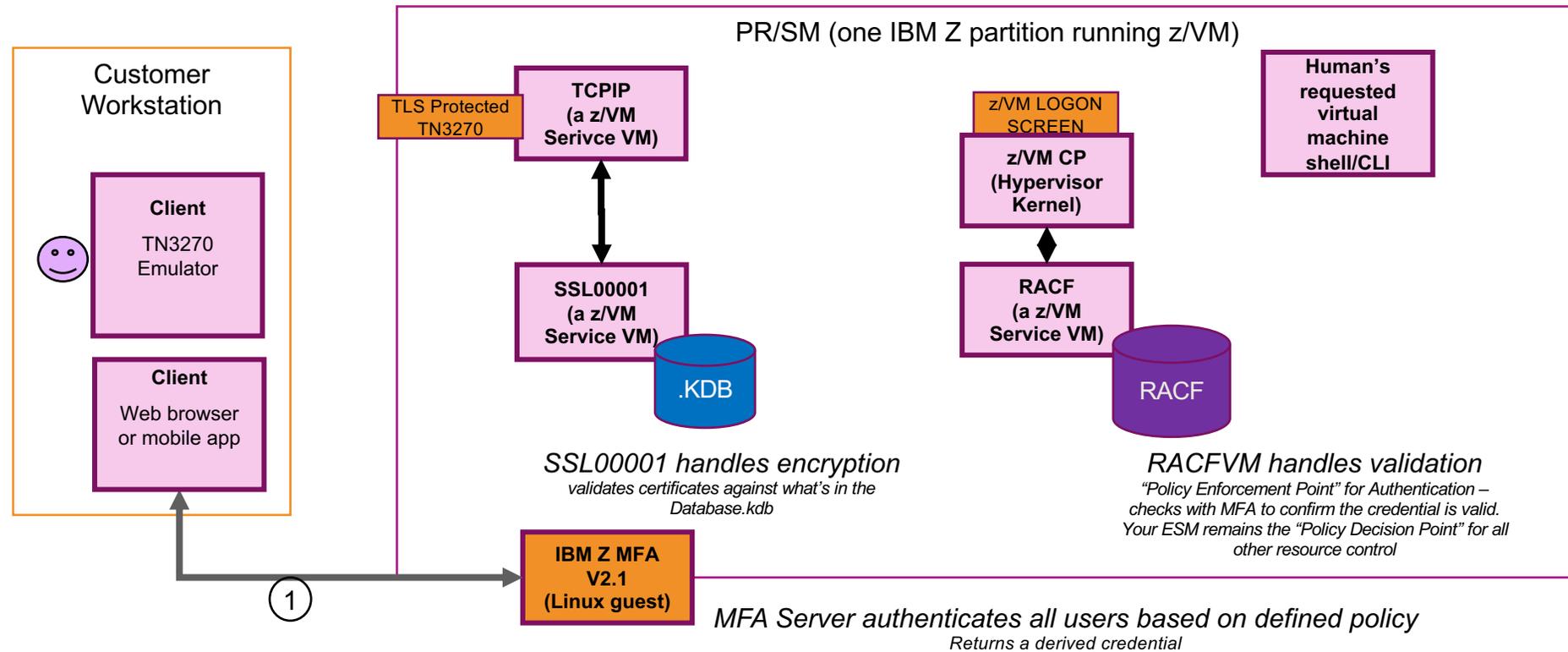
<https://www.vm.ibm.com/newfunction/#mfa>

- IBM Z Multi-factor Authentication V2.1 – a new priced product
 - Order through ShopZ
 - Yes, it'll say z/OS – don't panic. The Linux .iso will be available for download

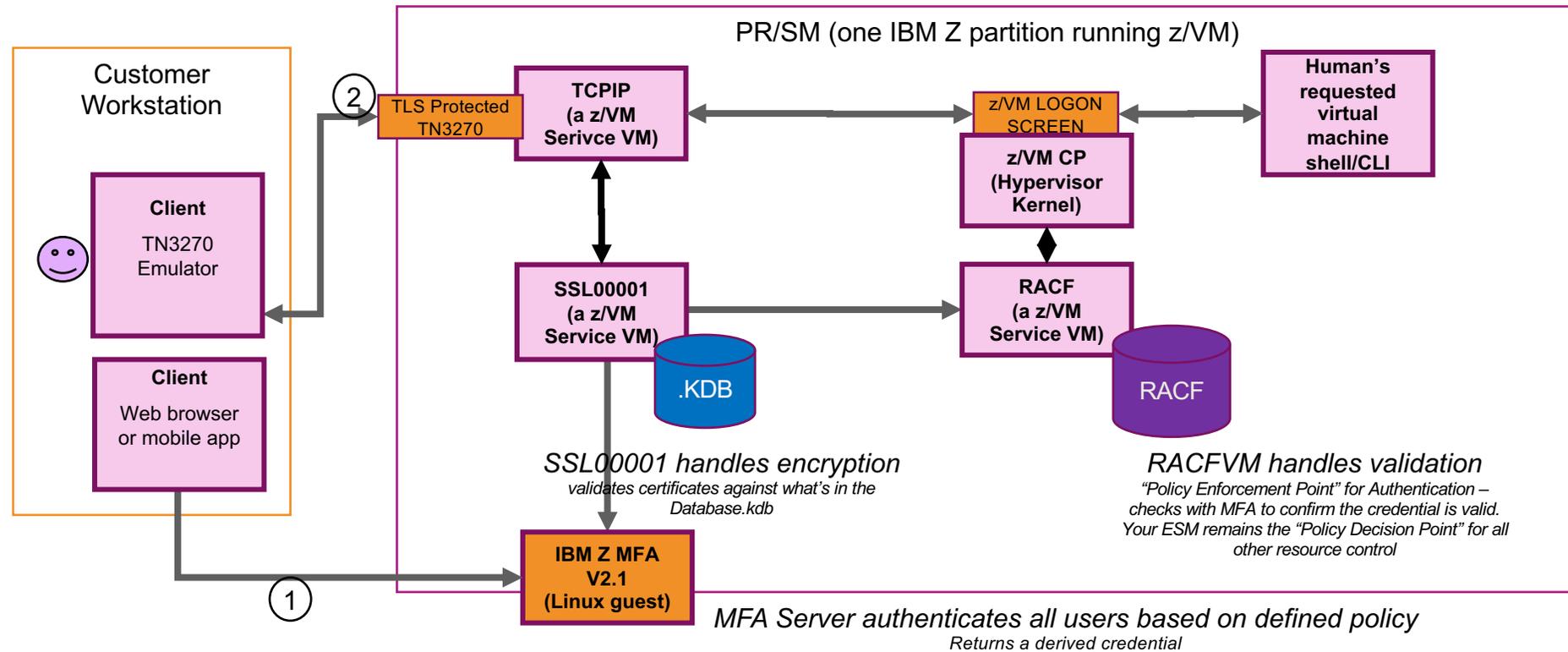
- For more information:
 - “Preparing for Multi-Factor Authentication on z/VM” presentation (recorded live at the VM Workshop):
<https://www.youtube.com/watch?v=AFkOtgEZxAc>

Component	APAR	PTF	RSU
CP	VM66324	UM35569	TBD
RACF	VM66338	UV99363	TBD
CA VM:Secure	CA VM:Secure 3.2 with the following required PTFs: <ul style="list-style-type: none"> • SO11972 - CA VM:Secure 3.2 - RSU-2001 - Recommended Service • SO12552 - ENH: Multifactor Authentication (MFA) support 		

Authentication Flow: z/VM with Multi-factor Authentication (1/2)



Authentication Flow: z/VM with Multi-factor Authentication (2/2)



9. Encrypt Sensitive Data

- **See #2:** know your data

- Encrypt it when it moves from place to place (**see: #4, #10**)

- Encrypt it when it's resident in memory, where you can
 - **dm-crypt** in Linux
 - **Dataset encryption** in z/OS
 - **RACF database for passwords and passphrases**
 - **Encrypted Paging** (when running on a z14 or later)

- Encrypt it when it's out on your storage volumes (**DS8880** and similar storage units)

10. Treat your virtual networks with care

- You should be using the z/VM Virtual Switch for Layer 2 routing between guests on a single z/VM partition
 - With guests using TLS to encrypt data leaving the virtual machine
 - With separation of traffic enforced as pertinent, from basic separation through VEPA
 - With ESM control of guest access to Virtual LANs
 - With a security decision being made (read: firewall) when data crosses network segments
 - Firewalls on a physical switch are fine
 - No need to waste the MIPS by putting this on z/VM itself

- Have you double-checked your defaults? Can your guests add themselves to networks, or create transient Guest LANs?
 - **See #3**

- How are your IUCV settings? How prevalent is IUCV ANY? **See #3**

- Are there controls around Hipersockets access?

- *Are there geographic regulations on relocation of guests onto another CPC?*

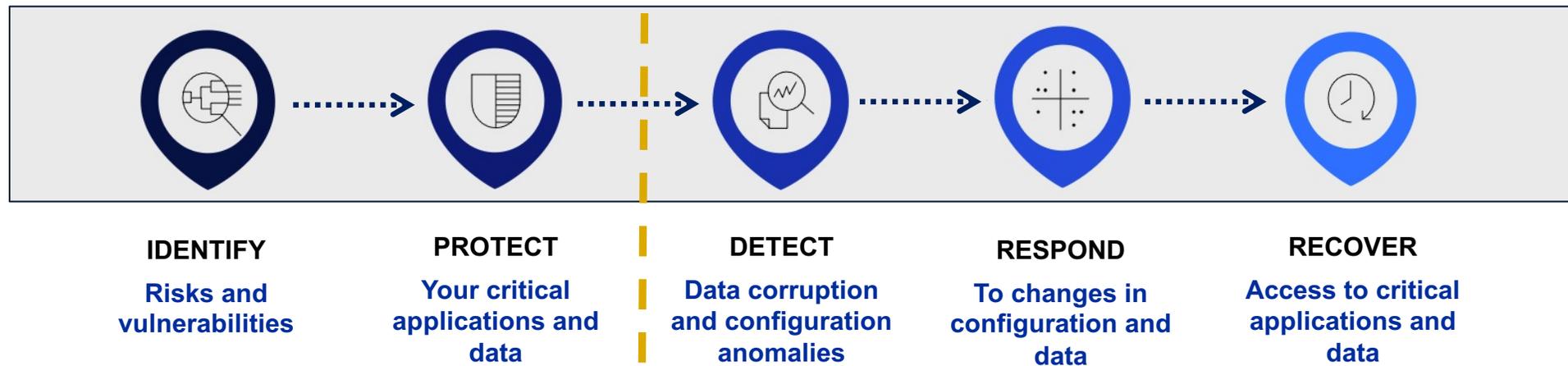
- [Do you still have that diagram for where your data is flowing?](#)

10. Treat your virtual networks with care

- Your inter-VM traffic can be as “separate” as your rules require (**see #1**)
 - Basic Vswitch connectivity, no virtual lans
 - Vswitch access with multiple lans
 - Vswitch access with Port Isolation, to force traffic to consider the OSA ports
 - Vswitch access with VEPA mode, to force traffic out to a physical switch before a “security decision” is made (read: there’s a firewall)
 - Use Directory Network Authorization (DNA) if you’re not already
 - Simplify management
 - Your VLANs, if you need them, should be backed by your ESM
 - [If not for the controls, then for the auditing](#)

11. Do you have a recovery plan?

- Security is defined as a combination of data confidentiality, system integrity, and service availability
- If your system ceases to be available (via hardware error, programmer error, intern pulled the wrong plug, meteor...) – How long will it take to recover your system?
- Are you making data backups (of sensitive data or otherwise)? Are those backups protected?



12. Now, set a timer.

- This may be Rule-dependent (#1)

- But however long it's for, when it pops... revisit these decisions

- The security landscape is changing continuously, and changing quickly

- Yesterday's "secure enough" is tomorrow's "broken"
 - That might move more slowly on IBM Z
 - But it's still true

Suggested Practices

Best Practice – Identity Management

- **Humans** need to prove who they say they are when authenticating to an information system. Only humans should be prompted for passwords (or other authentication tokens).
- Managing access—general authentication, levels of authorization—is vital to ensuring that your system is not modified improperly.
- Being able to prove it? Even more important.
- **Brian recommends:** a z/VM External Security Manager; IBM Z MFA; LDAP if pertinent across the enterprise; use of LOGONBY and SURROGAT for access to privileged virtual machines; a robust auditing policy

Best Practice – Authorization and Least-Privilege

- **Any virtual machine** (and by extension, the humans logging into them) should only have enough privilege to do their jobs—no more, no less
- z/VM comes “pre-packaged” with seven default privilege classes. More can be defined.
- An External Security Manager allows for granular access to all system resources and security-relevant commands
- **Brian recommends:** user-defined privilege classes for (a) Linux workloads / applications, and (b) administrators; ESM-defined privileges for access to specific resources—especially in cases where human jobs (e.g. network admin, storage admin) require separation of authorization between admins

Best Practice—Encrypt Sensitive Data

- Confidentiality is ensuring that only authorized personnel can see the data you want them to see
- Encryption is key to enforcing that separation
- Your regulations (internal/external/geo/industry/gov) may have specific requirements, both for data-in-flight and data-at-rest
- **Brian recommends:** z/VM TLS Server (data in flight), z/VM Encrypted Paging, Dynamic Vary Crypto for hardware-to-guest support, openssl and dm-crypt, DS8880 (for encryption of storage), Encrypted Tape...

Best Practice—Audit, Audit, Audit

- If you can't prove it happened, did it happen?
- If you can't prove who did it, who's responsible?
- Auditing may seem like busy-work (sort of like commenting code); but it can be what allows for problem determination and incident response to happen in a smooth and meaningful fashion
- **Brian recommends:** monitor records, ESM audit logs, and analysis of same.

**Questions? Comments?
(Time for a nap?)**

Summary

- Security can be a scary topic, but z/VM has a lot of features to offer

- “We can only show you the door. You’re the one who must walk through it.”

- Measure twice, cut once
 - Know your rules
 - Know the technology, and know where the data is going
 - Know how to “prove it” and meet audit requirements
 - Know how to recover in an emergency
 - Know when it’s time to change security posture

For More Information ...

- **z/VM New Function Page and Sponsor User Program:**
<https://www.vm.ibm.com/newfunction>
- **z/VM Security Page (new and improved!):**
<https://www.vm.ibm.com/security>
- **IBM Z Multi-factor Authentication for z/VM Manual (SC27-4938-40):**
[https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zMFAv210sc274938/\\$file/azfv100_v2r1.pdf](https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zMFAv210sc274938/$file/azfv100_v2r1.pdf)
- **“Preparing for Multi-Factor Authentication on z/VM” presentation (recorded live at the VM Workshop):**
<https://www.youtube.com/watch?v=AFkOtgEZxAc>

Contact Information:

[Brian W. Hugenbruch](#)

IBM Z Security for Virtualization & Cloud

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

 **[@Bwhugen](#)**

CISSP®



