#SHAREorg

SHARE
Technology · Connections · Results

The HMC Is a Fantastic Tool But Are You Making it Secure?

Barry Schrager
Xbridge Systems, Inc.

&

Paul R. Robichaux
NewEra Software, Inc.

Monday, February 5 at 12:15 pm

Session Number 12255

Plaza B

Insert Custom Session QR if Desired.

SHARE in San Francisco 2013

Abstract and Speakers

- The Hardware Management Console (HMC) is a fantastic facility that allows an installation to configure and dynamically reconfigure the LPARs in one or more zEnterprise Systems. But the HMC can also issue operator commands, bypassing Best Practice External Security Manager (ESM) procedures.

- It used to be that this kind of physical access was severely restricted because you had to be in the “Computer Room” to get to the console. But, now, this old kind of access plus the ability to change configurations, and even do it remotely, is available to many.

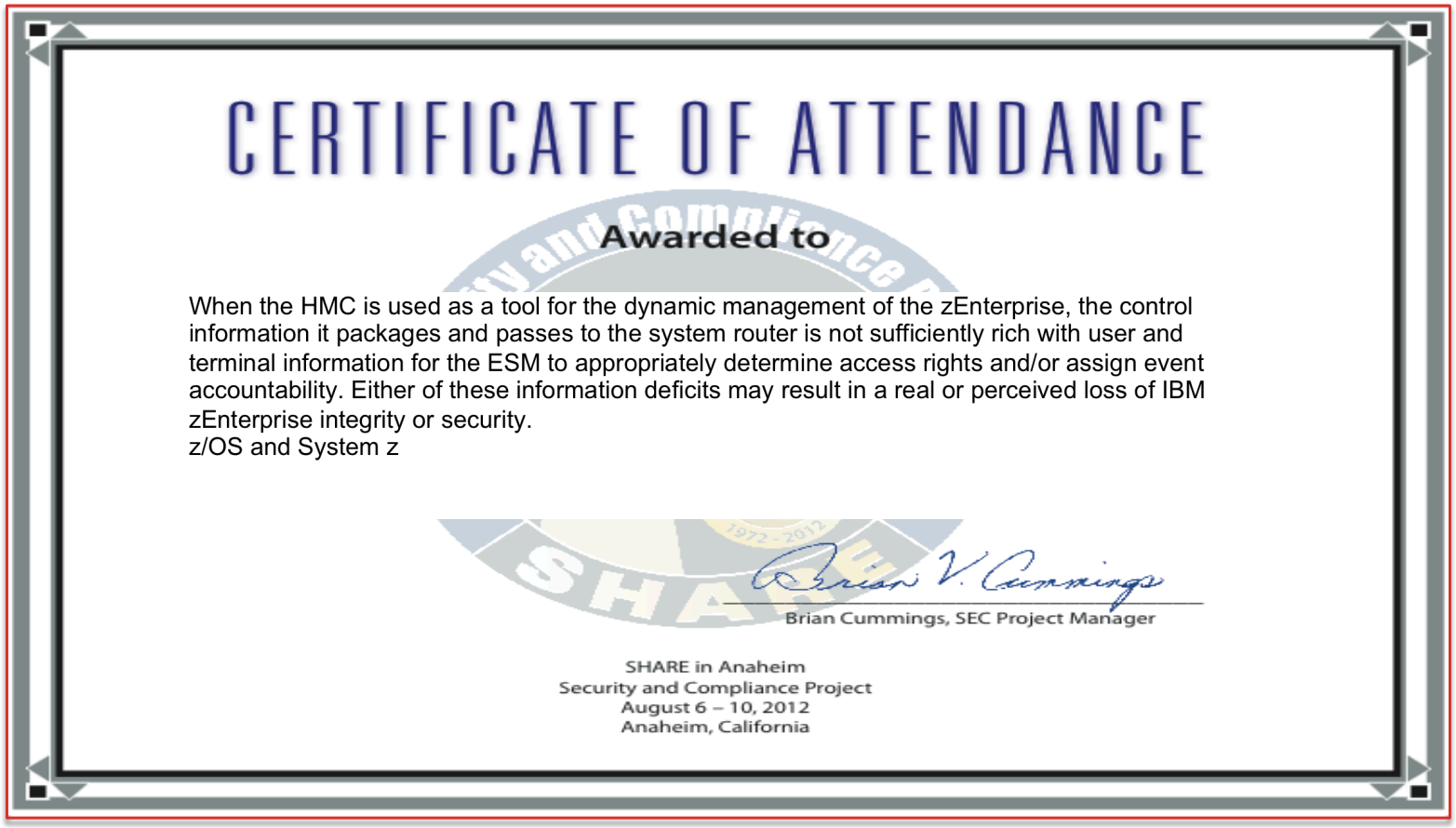
- This presentation will provide insight into HMC Control Issues, for example:

  - ✓ Can you vary a storage volume online from the HMC? – sure!
  - ✓ Can you add an APF authorized library? – sure!
  - ✓ How many people have authorized access to the HMC? 25, 50, 150?
  - ✓ Can they access it remotely? Do they need a Digital Certificate to do that?

- Barry Schrager was the first Project Manager of the SHARE Security Project. He is creator of ACF2, a member of the Mainframe Hall of Fame and currently President of Xbridge Systems. He holds a BS Degree in Physics from the University of Illinois and a Masters in Applied Mathematics from Northwestern University.

- Paul R. Robichaux, CEO, is co-founder of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University and is a Certified Public Accountant.

Continuing Education Credit



CERTIFICATE OF ATTENDANCE

Awarded to

When the HMC is used as a tool for the dynamic management of the zEnterprise, the control information it packages and passes to the system router is not sufficiently rich with user and terminal information for the ESM to appropriately determine access rights and/or assign event accountability. Either of these information deficits may result in a real or perceived loss of IBM zEnterprise integrity or security.
z/OS and System z

Brian Cummings, SEC Project Manager

SHARE in Anaheim
Security and Compliance Project
August 6 – 10, 2012
Anaheim, California

The Hardware Management Console

The HMC is a great Tool but…

- It can lead to an opening of system vulnerabilities
- These can be exploited to bypass Security Best Practices
- You need to know both how to use it and secure it.

Complementary Sessions…

- Session 12255 - will cover why you need to secure your HMC
- Session 12807 - will cover how you secure your HMC

Brian Valentine, IBM
HMC Security Basics and Best Practices
Tuesday, February 5 - 3:00 PM
Franciscan D

A Statement of the Problem

HMC Security Vs. zEnterprise Integrity and Security

- It is a common z/OS Security best practice to seek full accountability; user, terminal and action identification of events that are intended to modify the functional configuration - the hardware and software of the IBM zEnterprise.
- Functional control over resource access and resource use is provided by the External Security Managers (RACF, CA ACF2, CA Top Secret) and is dependent on this vital information in maintaining the integrity of the IBM zEnterprise environment.
- When the HMC is used as a tool for the dynamic management of the zEnterprise, the control information it packages and passes to the system is not sufficiently rich with user and terminal information for the ESM to appropriately determine access rights and/or assign event accountability.
- This information deficit results in a loss of zEnterprise system integrity and security from the perspective of the External Security Manager and the Security Professionals that depend on its oversight and reporting.

Presentation Outline

Session 12255 Outline:

- HMC - Security Concerns:
  - *The Good Old Days*
  - *Basic Control Issues*
  - *What Users are Reporting*
  - *Can you Pass this Compliance Test?*
  - *What's Right for Your Organization?*
- HMC - Fantastic Tool:
  - *What is it?*
  - *How does it work?*
  - *Where is it going?*
  - *Vulnerability?*
  - *Beyond the HMC?*
- HMC – Recommended Best Practices

HMC - Security Concerns

The HMC does introduce some Security Concerns

- *The Good Old Days*
- *Basic Control Issues*
- *What Users are Reporting*
- *Can you Pass this Compliance Test?*
- *What's Right for Your Organization*

HMC - Security Concerns

In the good old, golden days…

- Consoles were located where the Operations personnel worked
- This was almost always secured by locked doors and passkey access
- Operators would notice who was walking around
- And who was doing something at the console
- And often look over their shoulder while they were doing it

HMC - Security Concerns

A Statement of Requirements - FFEIC

Financial Institutions should secure access to the operating systems by:

- Securing the devices that can access the operating system through physical and logical means
- Restrict operating system access to specific terminals in physically secure and monitored locations

Source: Federal Financial Institutions Examination Council (FFEIC)

http://ithandbook.ffiec.gov/it-booklets/information-security/security-controls-implementation/access-control-/operating-system-access.aspx

HMC - Security Concerns

z/OS Supports Console Logon and Provides the Ability to:

- Force a user to logon to consoles although it could be set to automatically log them on with a defined Userid
- Authorize commands entered via ACF2, RACF or Top Secret based upon the Userid of the Operator who logged on to the console

But the HMC Does not Support these z/OS Control Features:

- Commands entered from the HMC pass to ACF2, RACF and Top Secret with the same Userid for ALL HMC's
- All commands have the same Userid – that of the Console name as specified in the Console member of PARMLIB
- There is no way for the ESM to distinguish one user from another or one HMC to another

HMC - Security Concerns

The HMC is Powerful Medicine – From the HMC you can

- Dynamically reconfigure your LPARs
- Issue Operator Commands, e.g.
  - VARY xxx,ONLINE
  - SETPROG APF
  - MODIFY
  - ACTIVATE
- Select IODF Components - IOCP and OSCP
- Specify LOADxx Configurations
- And of course, POR and IPL your LPARs

HMC - Security Concerns

The HMC is Powerful Medicine – From the HMC you can

- Configure a “sandbox” LPAR – or use your test/development LPAR (usually people have higher authorities there)
- Use an IODF that mapped production storage volumes to it (normally these would be varied offline or, more securely, not even mapped to the sandbox LPAR)
- Vary a production volume online to the “sandbox” LPAR
- Look at (or modify) any sensitive production data
- Or, add a “bad” APF authorized program to a production APF authorized library

HMC - Security Concerns

The HMC is Powerful Medicine – For Example You Could - 1,2,3

1. Issue SETPROG APF command for your own library on a Production LPAR.
2. Link Edit a program marked AC(1) into the library.
3. The Program is now an APF Authorized Program.

The Resulting Authorized Program Could Then:

1. MODESET KEY=ZERO to get into protect KEY ZERO.
2. Modify its identity to make ACF2, RACF or Top Secret think the program is a Super or a Production user or “owned” the production dataset you want to modify
3. Now with full access to Production Data, have your way.
4. You could modify any dataset you wanted to without any interference from the External Security Manager

HMC - Security Concerns

The Basic Control Issue – Lack of Accountability

- A User Identifier, i.e. Userid is not passed along to z/OS
- The Userid passed to z/OS is the Console Name of the main HMC

So What?

- All HMC users and HMC devices look the same to z/OS
- Therefore:

  The External Security Managers (ACF2, RACF, Top Secret), using their OPERCMDS Facility Class, are unable to adequately enforce Best Practice, user by user, terminal by terminal control over dynamic z/OS system updates and changes.

HMC - Security Concerns

Do these HMC User Reports make you feel comfortable?

- My remote access works both from behind the firewall, and VPN from home or on the road.
- It even works with a wireless modem on the Amtrak going south from Irvine to San Diego the day after it was installed.
- We use HMC Role Assignment Defaults and assume that all activity generated from the HMC is by a vetted user.
- I can't get my Operations and Systems people to cooperate with me (the RACF Security Guru) on controlling access within the HMC.

Source: Posted on bit.listserv.ibm-main or HMC user interviews

HMC - Security Concerns

How would your organization score on this Compliance Test?

- ❑ Where is your HMC located?
- ❑ Who can walk up to it?
- ❑ Which users are defined to it?
- ❑ Do they all have the same high level authority?
- ❑ Can it be accessed remotely?
- ❑ Which users can access it remotely?
- ❑ Are they defined to require a digital certificate?
- ❑ Does anyone, even occasionally, review the logs?

HMC - Security Concerns

How many people have access to your HMC?

- 15, 30, 45, 100, 150?
- Do you even know who they all are?
- Are they employees of your Outsourcer?
- Do you know who they are? Have you vetted them?

What's the right number?

- Only you can decide that, but the lower the number, the lower the risk.
- Do they all have the same powerful privileges?
- Can they **all** access it remotely?
- Is that really necessary?

HMC - Security Concerns

Remote Access Recommendation – IBM System z HMC Security

- Unless absolutely required, make sure that remote access to the HMC is disabled.
- When remote access is required, make sure to allow such access only for the specific user IDs that require it.

Source: https://www-304.ibm.com/servers/resourcelink/lib03011.nsf/pages/zHmcSecurity/$file/zHMCSecurity.pdf

HMC - Fantastic Tool

The HMC as The zEnterprise Manager

- *What is it?*
- *How does it work?*
- *Where is it going?*
- *Vulnerability?*
- *Beyond the HMC?*

HMC - Fantastic Tool

Hardware Management Console (HMC) – How Secure!

It's not that the HMC is either:

- Insecure or
- Offers no Security Controls.

It's just not the kind of Security that you're:

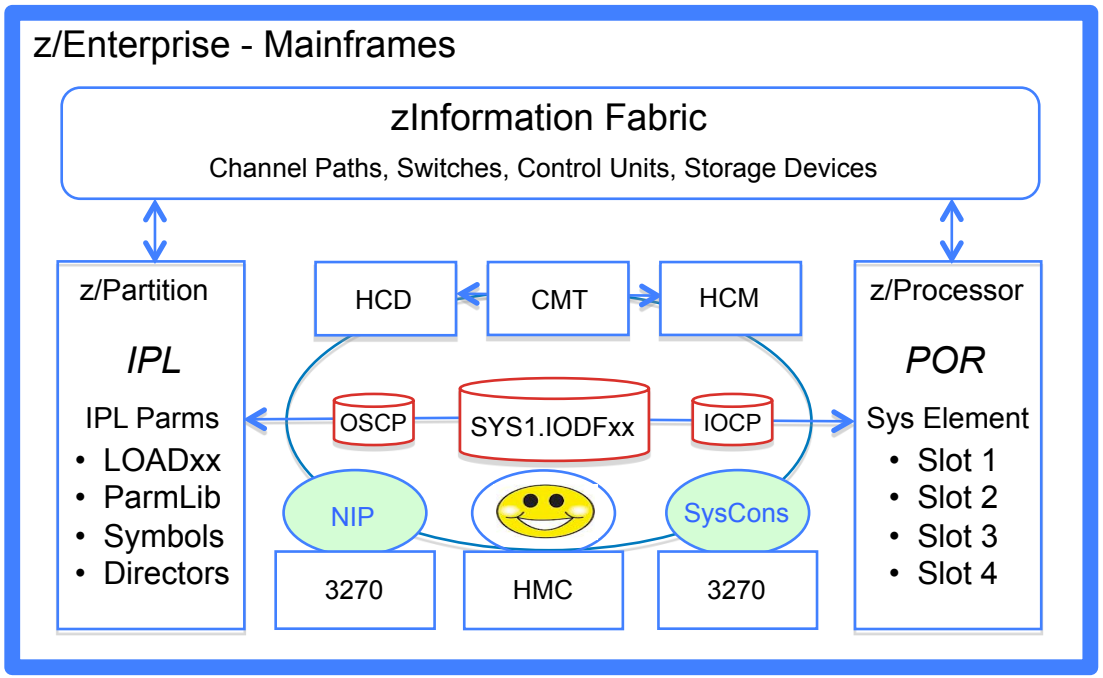
- Thinking of or
- The type of ESM Security[1] you are used to.

[1] *Resource and/or Access Security of the type provided by CA ACF2, RACF, CA Top Secret*

HMC - Fantastic Tool

Hardware Management Console (HMC) – It's Simple, Don't get Confused!

- You can operate a z/OS system or an entire Sysplex using the *Operating System Message Facility* of the HMC. This facility is also known as the SYSCONS console and is considered an Extended MCS type of Operator Console.
- You would generally only use this facility if there were problems with the CONSOLES defined with *Master Console Authority* in the CONSOLxx parmlib member.

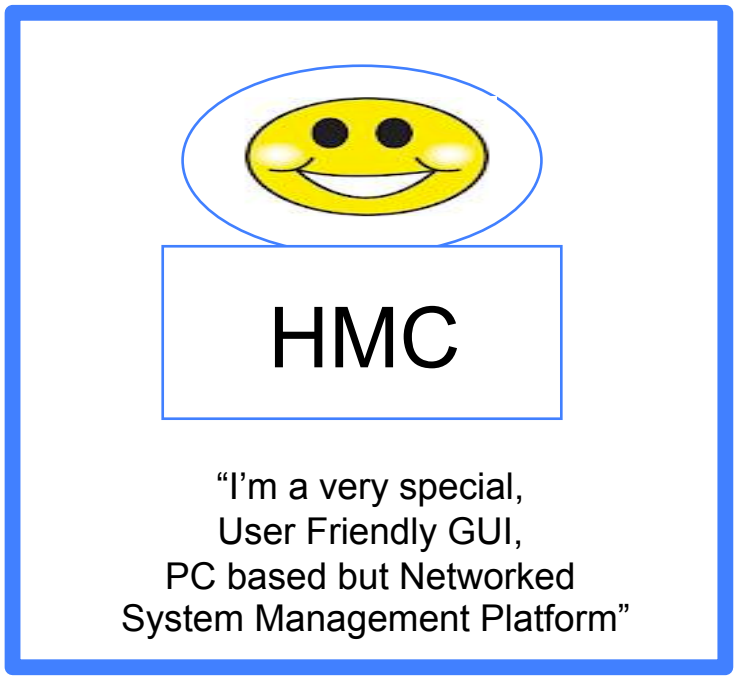


Source: System z:Hardware Management Console Operations Guide, SC28-6857-01

HMC - Fantastic Tool

Hardware Management Console (HMC) – What is it? – Part 1

- HMC is an acronym that describes the IBM technology that is used to manage and monitor IBM Mainframe and/or IBM UNIX servers.
- HMC is required before all the capabilities of a System zServer can be fully operational.
- HMC provides a GUI through which authorized operators manage configurations and partitions of zServer in a multi-system complex
- HMC monitors an individual system for hardware and other operational problems.
- HMC should be considered an appliance, meaning it's a *"Closed Platform"*.

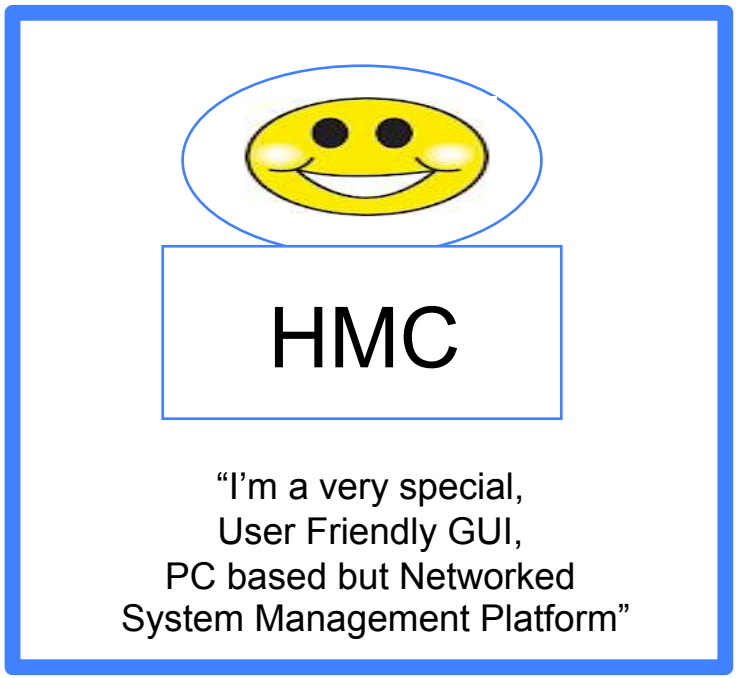


Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

HMC - Fantastic Tool

Hardware Management Console (HMC) – What is it? – Part 2

- HMC hardware is not serviced by the user, only IBM personnel perform this task.
- HMC is not an operating platform, not usable by an end user for other application execution.
- HMC uses a *"Private Network"* connection(s) to one or more zServer(s) Frames in order to perform management functions.
- HMC must be tested for network security using procedures that include periodic network scans to detect intrusion attempts.
- HMC monitors and logs the activity of its users based on their pre-assigned roles.

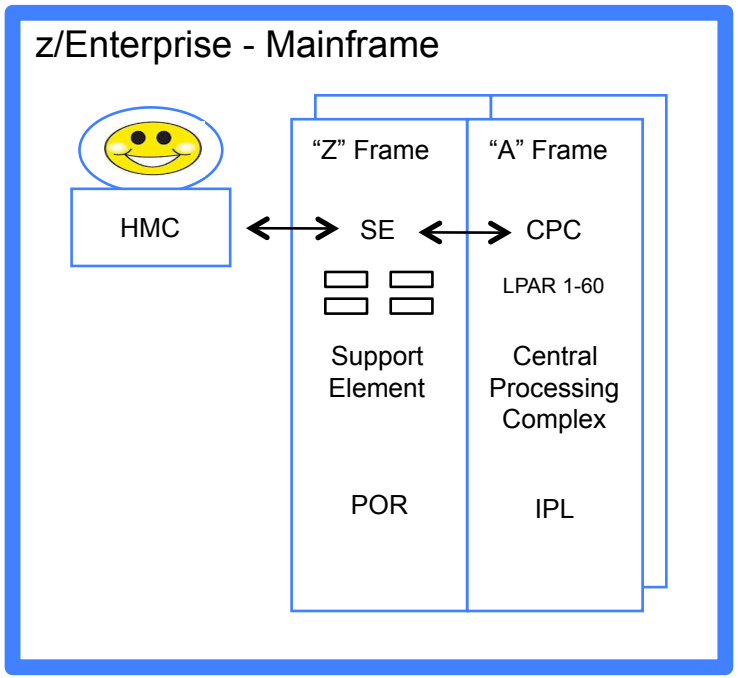


Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

HMC - Fantastic Tool

Hardware Management Console (HMC) – The Basics – Part 1

- SE - Regardless of what hardware is in a mainframe complex, it can be managed using the Support Element (SE) that is directly attached to the Central Processing Complex (CPC/CEC). The SE and/or HMC can perform such tasks as:
  - ✓ Configuring and Testing the hardware
  - ✓ Loading the Operating Systems
  - ✓ Concurrent repair
  - ✓ Concurrent upgrade
  - ✓ Reporting of and recovering from errors
  - ✓ Other Management tasks
- Each SE has four "Configuration Slots". Each Slot is loaded with an I/O hardware configuration defined in a Production Level IODF Dataset.

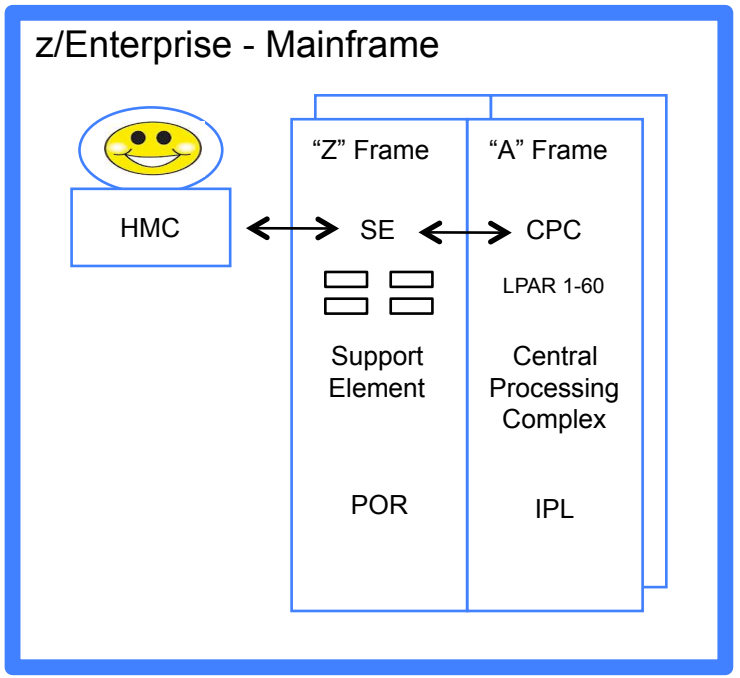


Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

HMC - Fantastic Tool

Hardware Management Console (HMC) – The Basics – Part 2

- The CPC may have up to 96 processors, 80 of which are devoted to production work and may be subdivided into up to 60 z/OS LPARs.
- HMC commands are sent to the SE; the SE sends these commands to a targeted CPC/LPAR.
- CPCs can be grouped at the HMC so that a single command can be passed along to all of a defined set of CPCs.
- HMC hardware commands, used in a Power-On-Reset (POR), are processed by the SE. MVS operator commands, used in an Initial Program Load (IPL), are processed by the individual Logical Partitions (LPAR) defined to the CPC.

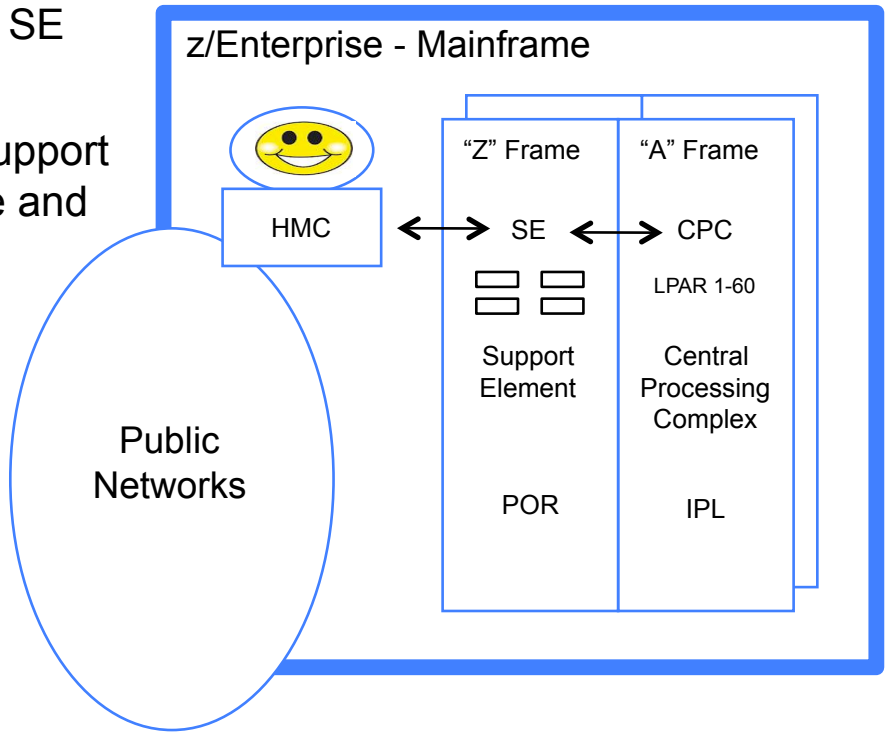


Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

HMC - Fantastic Tool

Hardware Management Console (HMC) – The Basics – Part 3

- HMC can control up to 100 SEs and one SE can be controlled by 32 HMCs.
- HMC can only communicate with CPC support elements that have the SAME domain name and domain password as the HMC.
- HCM can be operated remotely. Remote access via a Public (TCP/IP) Network is monitored and controlled as follows:
  - ✓ HCM User Role Logon Procedures Enforced
  - ✓ HMC Communication to SE is Encrypted
  - ✓ HMC Digital Certificates are Provided
  - ✓ HMC Remote Activity is Logged



Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 1

❑ To use the SYSCONS console on the HMC, select the Operating System Messages (OSM) task and the target system on the HMC. The HMC will open the SYSCONS console for the system.

To use the SYSCONS console for command processing first enter

```
VARY CN(*),ACTIVATE
```

This allow the SYSCONS to send commands in Problem Determination (PD) mode.

- *Almost any z/OS command can now be entered, with a few restrictions.*
- *Active system SYSCONS console may be accessed by multiple HMCs and*
- *It is not necessary to issue the VARY CONSOLE command for each HMC.*

The Active system SYSCONS remains active for the duration of the IPL, or until the

```
VARY CN(*),DEACT
```

command (to deactivate the system console) is entered.

HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 2

- Try this at Home – Display the Active Consoles ACTIVE using this command:

```
/DISPLAY CONSOLE,ACTIVE,CA
```

- The name of HCM Console(s) returned is the System Name/Id and NOT the Console Name. The HMC per se will not show up as an active console. It appears that System Name/Id is used for logging command issued from the HMC.

```
NC0000000 MAI2     2012123 13:34:56.98 MAI2     00000290  D C,A,CA

  LR                 291 00000090  CONSOLES MATCHING COMMAND: D C,A,CA
  LR                 291 00000090  NAME      TYPE  SYSTEM    ADDRESS   STATUS
  DR                 291 00000090  MAANXOCC  MCS   MAI2      10A2      ACTIVE
  DR                 291 00000090  MACN10A0  MCS   MAI2      10A0      ACTIVE
  DR                 291 00000090  MACR2080  MCS   MAI2      1080      ACTIVE
  DR                 291 00000090  MFANXOCC  MCS   MFI3      10A2      ACTIVE
  DR                 291 00000090  MFCN10A0  MCS   MFI3      10A0      ACTIVE
  ER                 291 00000090  MFCR2180  MCS   MFI3      1180      ACTIVE
```

Source: A Gracious project participant!

HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 3

❑ To determine whether a particular user (an operator) is allowed to access a particular resource (command or console) a security profile is used. The security administrator can define a security profile for:

- ✓ Each user of a console
- ✓ Each console that is to be automatically logged on
- ✓ Each MVS™ command issued from a console

If an installation's security policy requires an audit of operator commands according to the identity of the user, then all operators must be defined by individual user profiles.

These profiles define access – who can issue what command or use a specific console or terminal - and the level of security auditing required by site best practices.

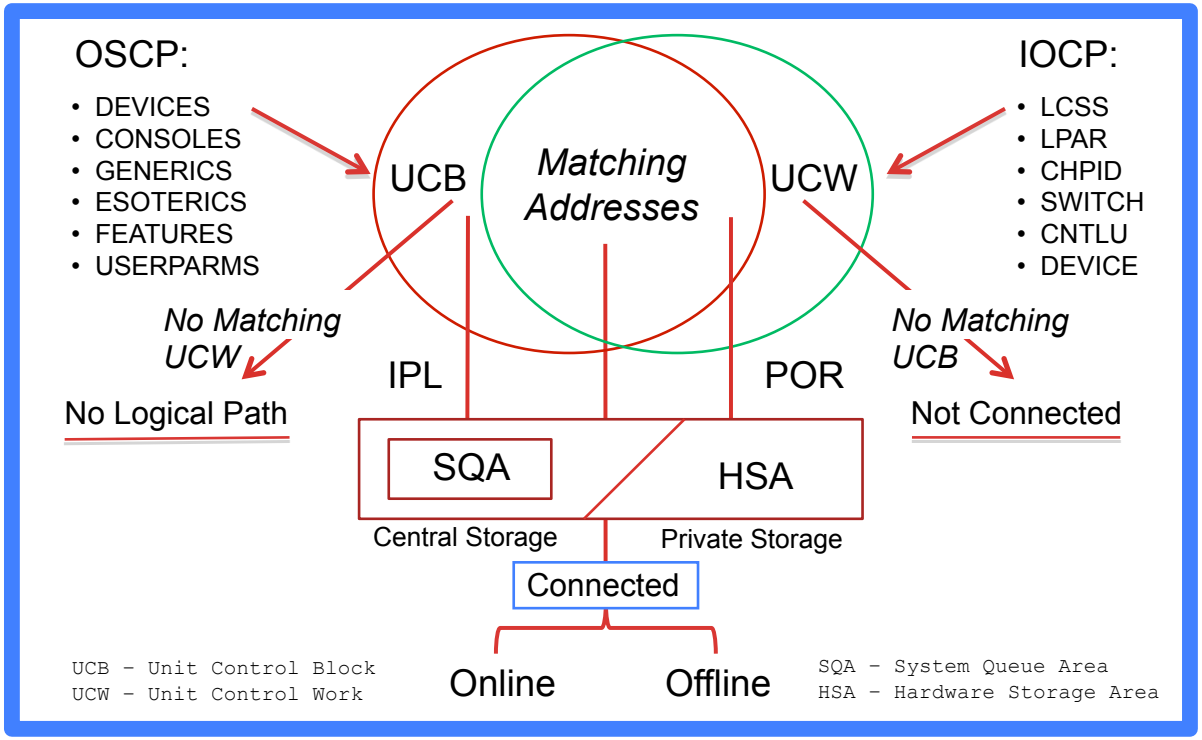
HCM events may not be sufficiently populated
with user and/or terminal identity
to satisfy these requirements.

Source: z/OS V1R11.0 MVS Planning Operations - SA22-7601-11

HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 4

- VARY - Use this Operator Command to make a device or ranges of devices available for allocation to problem programs and other system tasks.
- ACTIVATE - Use this command to activate a new I/O configuration definition dynamically.

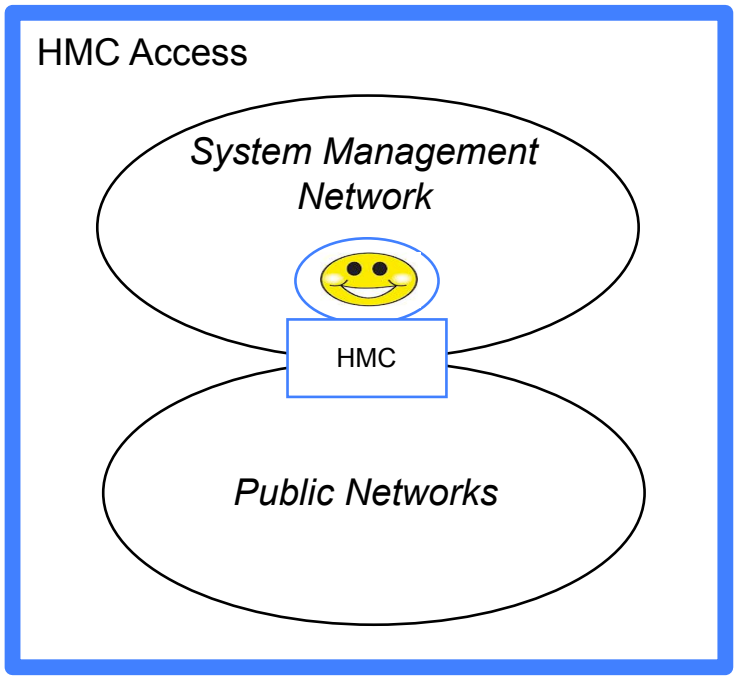


Source: z/OS V1R12.0 MVS System Commands - SA22-7627-24

HMC - Fantastic Tool

Know Your Environment – The Origin of Vulnerability – Part 5

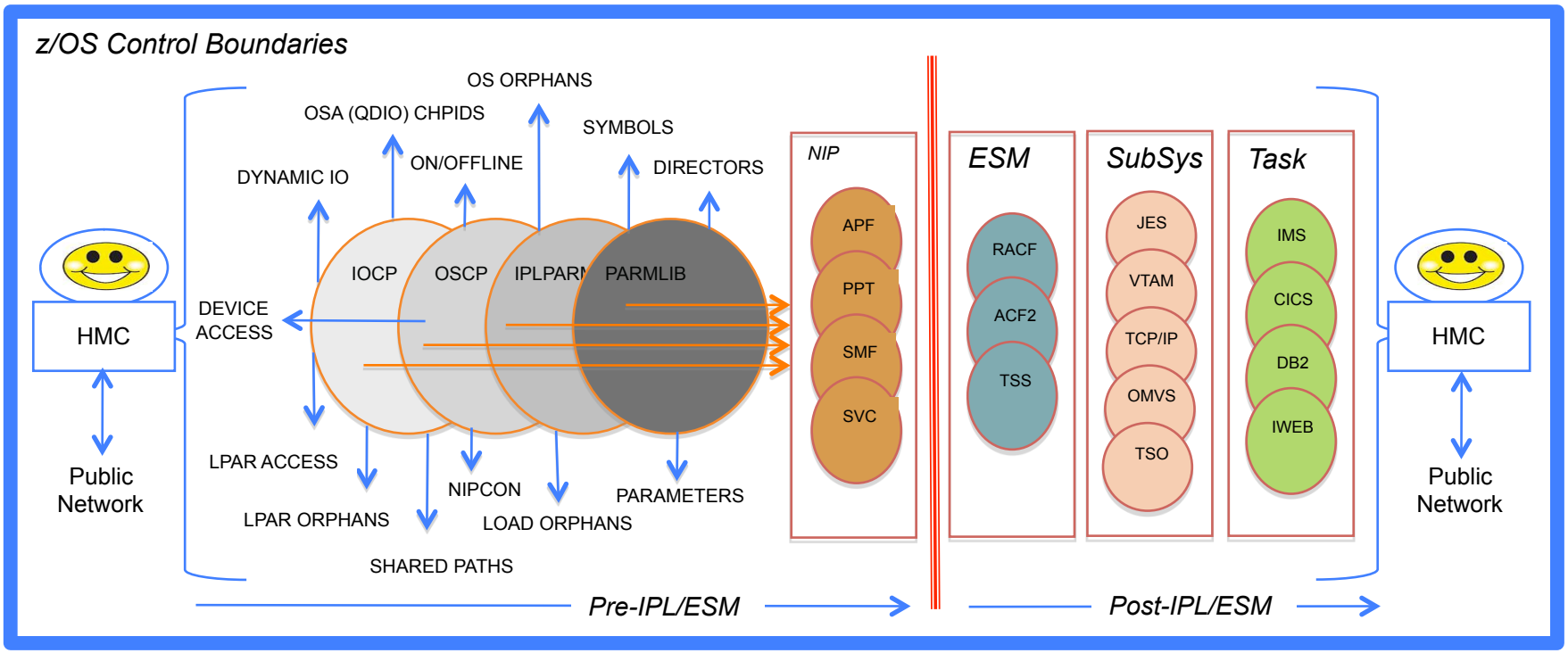
- A typical HMC network is a dedicated network on which only System z servers and HMCs are present. This network is separate from the other networks and network services, such as internet access. This dedicated network provides increased security because the server is not exposed to potentially dangerous traffic.
- However, in practice, HMCs are often configured with two network interfaces so that they can exist on both the dedicated network and a more general corporate network, thus allowing access to the HMC from anywhere the network exists, including the World Wide Web.



Source: Introduction to the System z Hardware Management Console, ibm.com/redbooks

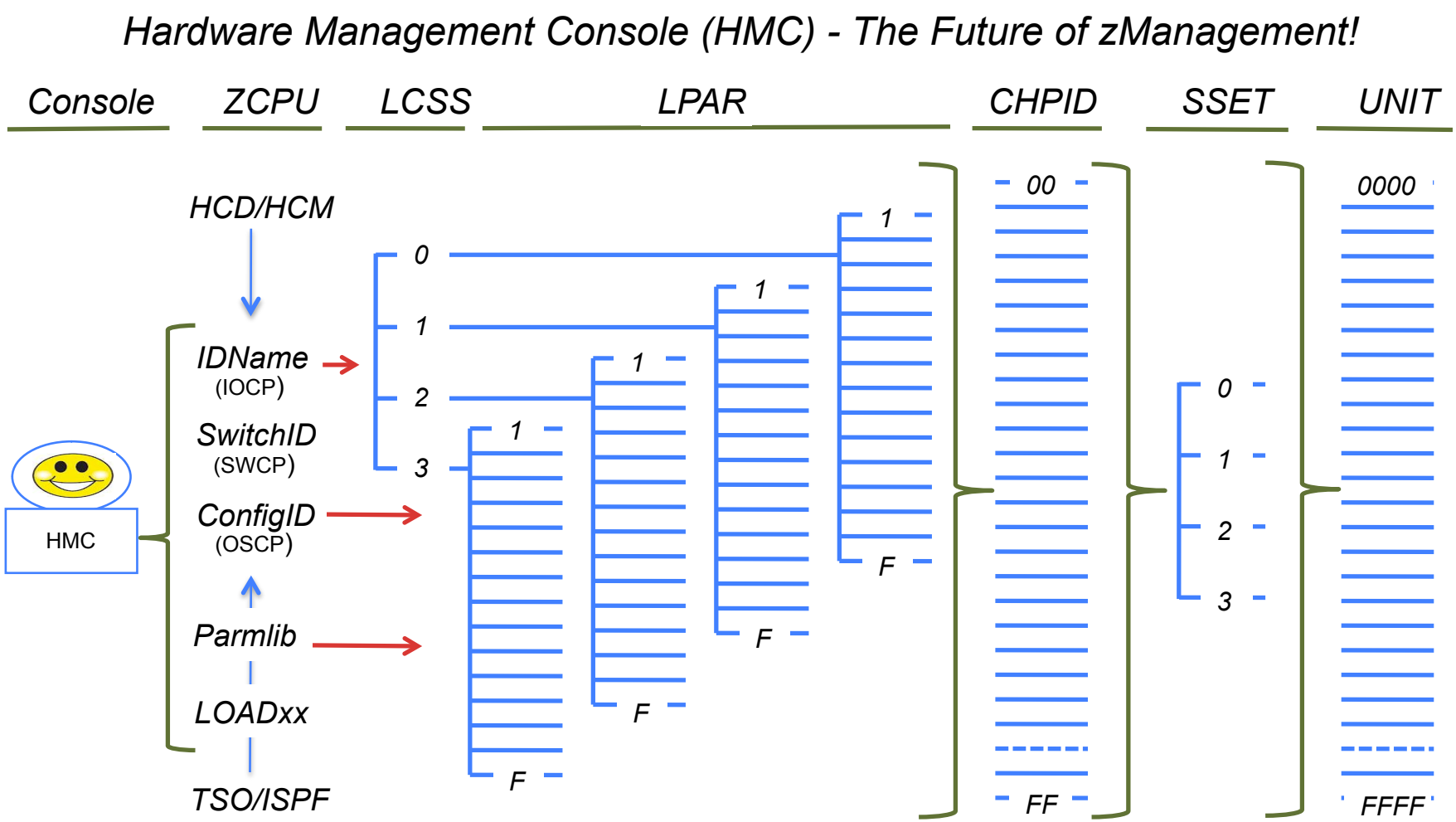
HMC - Fantastic Tool

Hardware Management Console (HMC) - It's Simple, Don't get Confused!



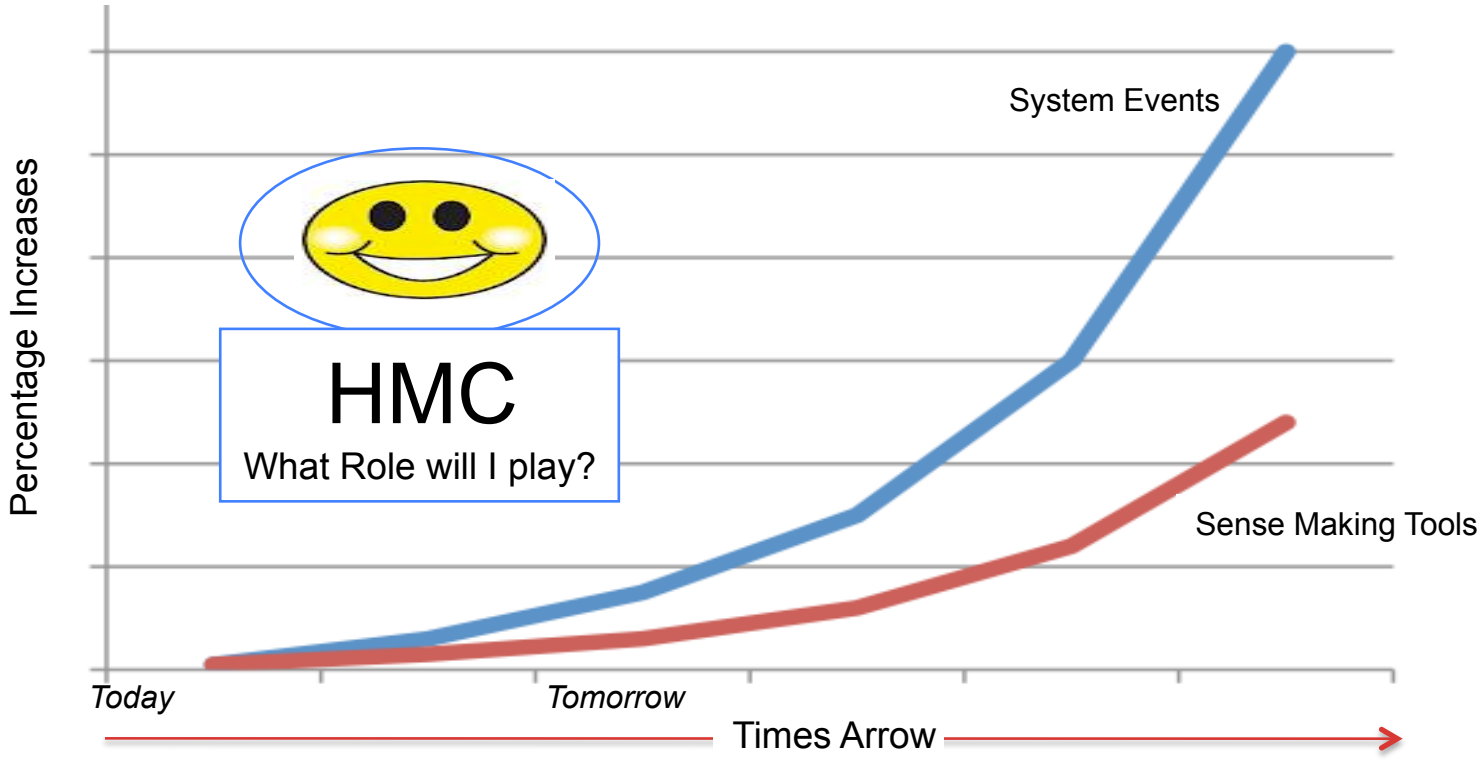
Source: Share, August, 2011, Session Number 10101 "IODF as the Foundation of z/Enterprise Compliance"

HMC - Fantastic Tool



HMC - Fantastic Tool

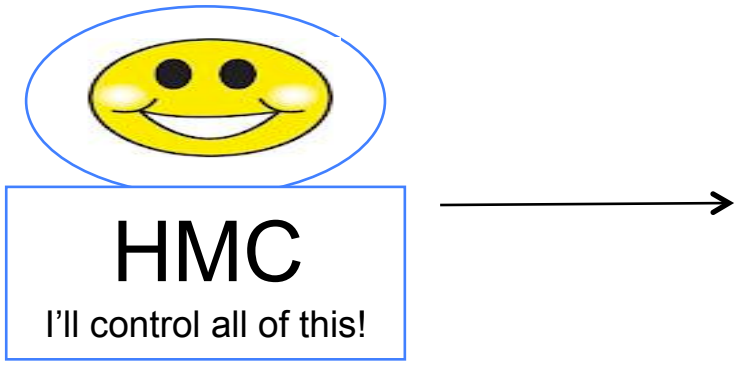
Hardware Management Console (HMC) - The Future of zManagement

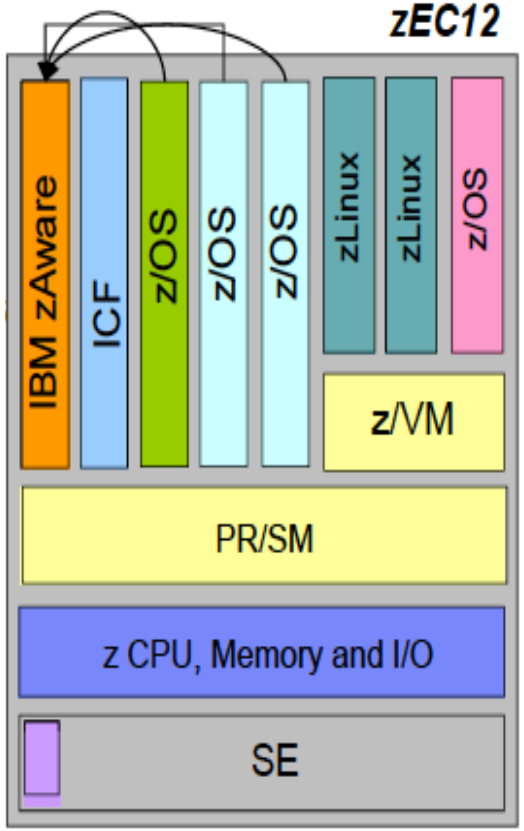


[1] *More than 40,000 unique message IDs are defined for z/OS and the IBM software that runs on z/OS systems.*

HMC - Fantastic Tool

Hardware Management Console (HMC) - The Future of zManagement





"You can operate a z/OS system or an entire Sysplex using the Operating System Message Facility of the HMC."

Source: System z:Hardware Management Console Operations Guide, SC28-6857-01

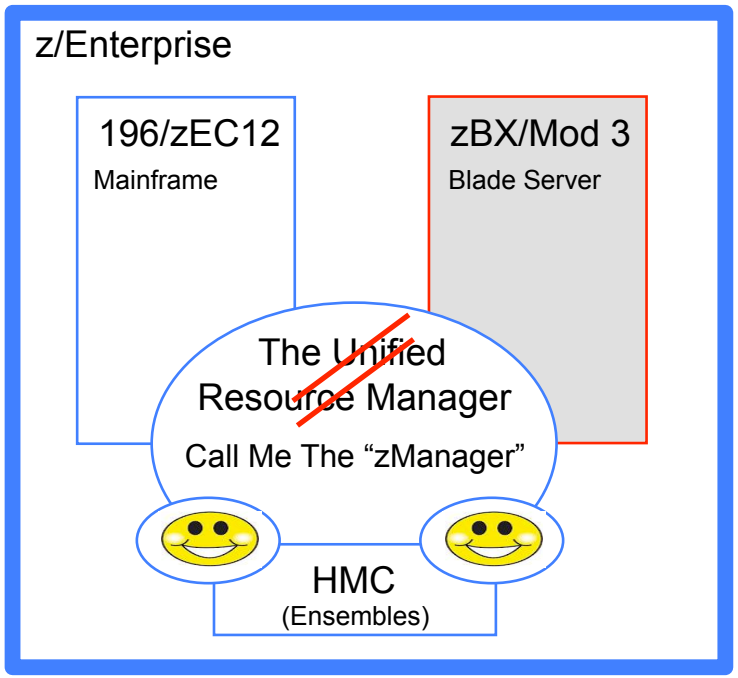
HMC - Fantastic Tool

Hardware Management Console (HMC) – The Future – Part 1

❑ Hyper-scale servers are designed for large scale datacenter environments where parallelized workloads are prevalent. The *Form-Factor* serves the unique needs of these datacenters with streamlined system designs that focus on:

- Performance
- Energy efficiency
- Platform Density

❑ Hyper-scale servers forego the full management features and redundant hardware components found in traditional enterprise servers as these capabilities are accomplished primarily through software.

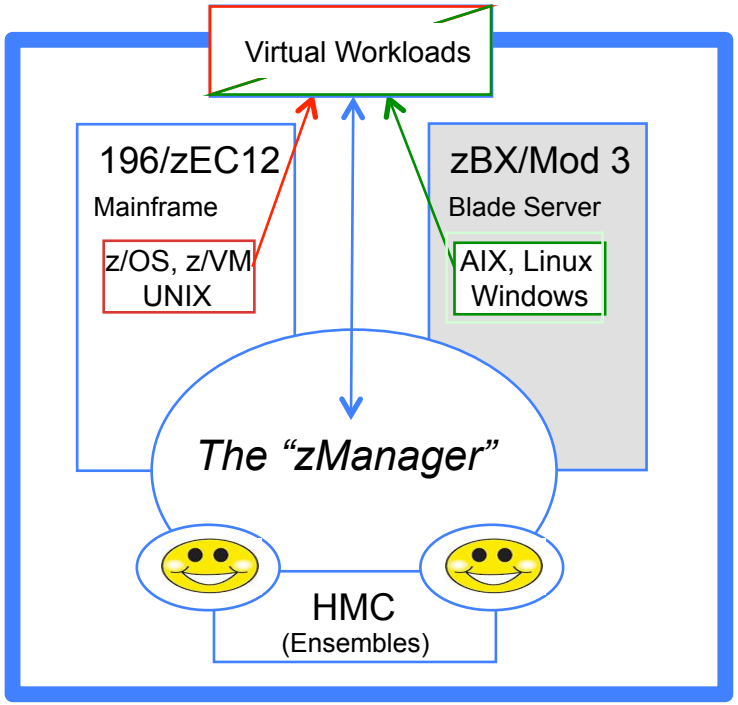


Starting Q3 2011, IDC began to track the new form-factor called hyper-scale servers.

HMC - Fantastic Tool

Hardware Management Console (HMC) – The Future – Part 2

- The integration of the hardware platform that brings mainframe and distributed technologies together will, over time, replace individual islands of computing. These integrated resources are called *Ensembles*.
- Each Ensemble will be managed as a single logical, "Virtualized" system by the URM, through the HCM. The HMC will create and manage ensemble resources.
- Some of the benefits of the ensemble:
  - ✓ Reduction of complexity
  - ✓ Improve security
  - ✓ Applications closer to needed data.

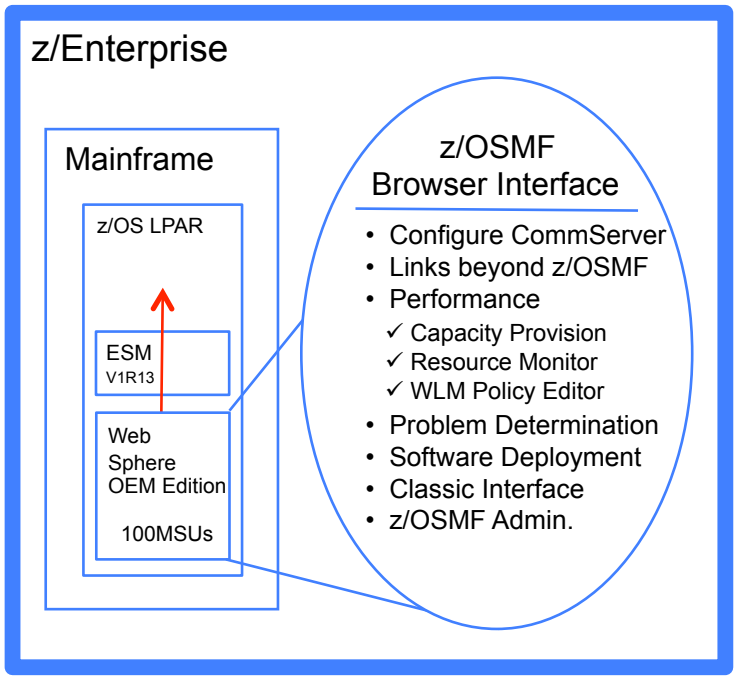


Source: zEnterprise Unified Resource Manager: Building an Ensemble, SG24-7921-00

HMC - Fantastic Tool

z/OS Management Facility (z/OSMF) - V1R11 – Beyond the HMC

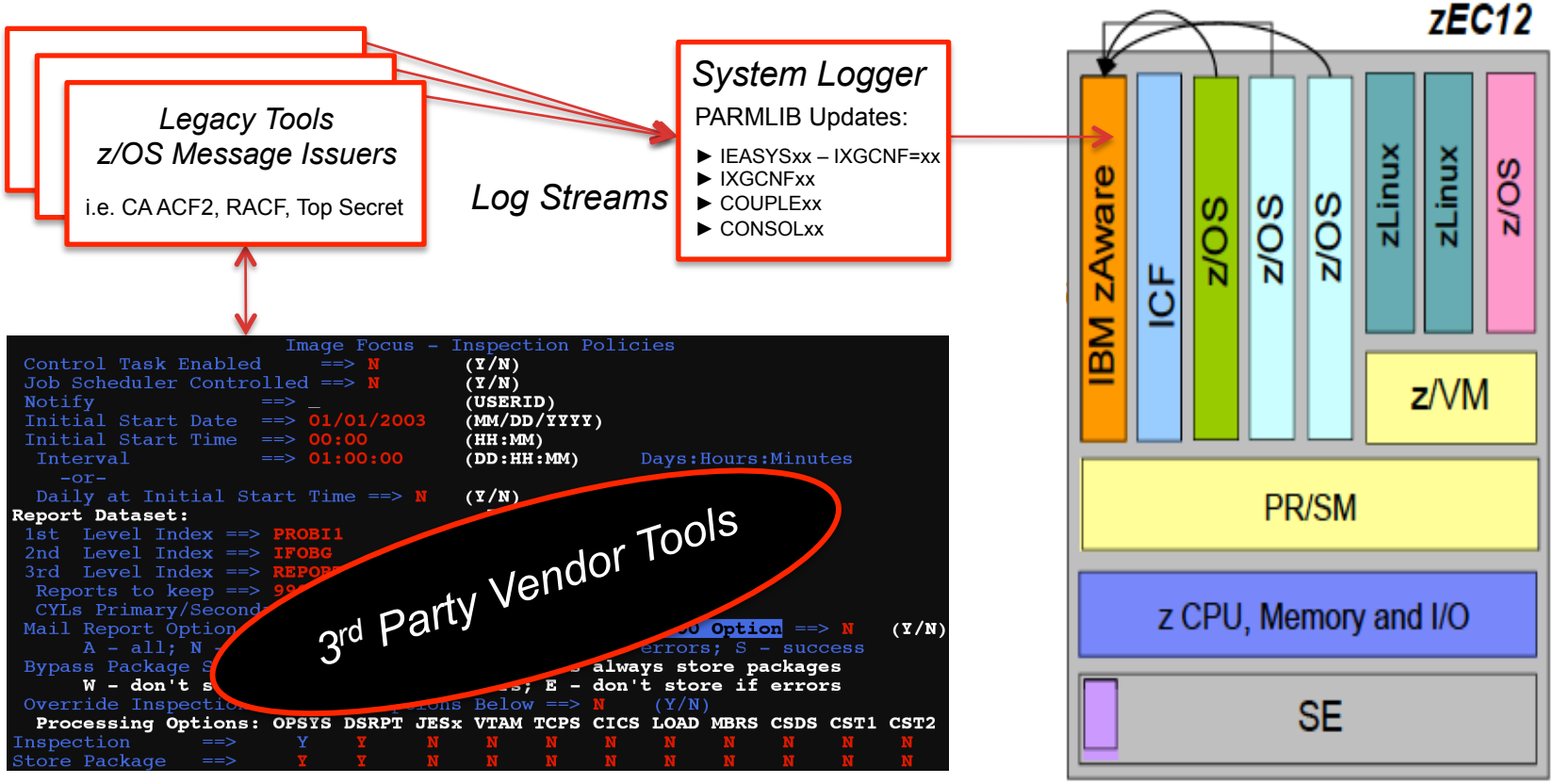
- ❑ Provides support for a modern, Web browser-based z/OS management console.
- ❑ Helps system programmers to more easily manage a mainframe system by simplifying day to day operations and administration of a z/OS system.
- ❑ z/OSMF provides the intelligence needed to address the requirements of a diversified workforce, maximizing their productivity.
  - ✓ Automation reduces the learning curve and improves productivity.
  - ✓ Embedded assistance guides activities and simplifies operations.



Source: SHARE Seattle, Session 2249 – Greg Daynes & Anuja Deedwaniya

HMC - Fantastic Tool

Hardware Management Console (HMC) – The zManager - zAware



[1] *z/U 04/2012 - zZS18: Smart Monitoring of z/OS with IBM zAware on zEC12 by Riaz Ahmad*

HMC – Fantastic yes, Secure?

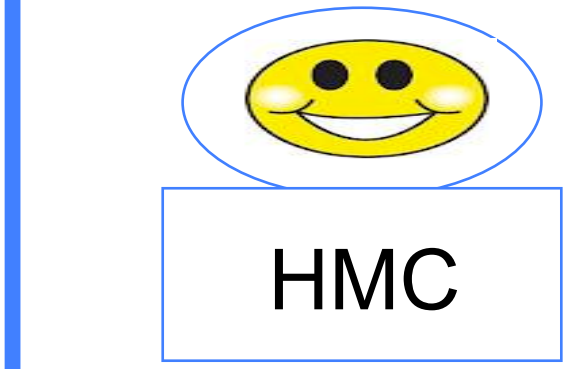
So What's the Conclusion - Do you like me now?

- You may have taken a very secure interface to z/OS

  …users had to be in the room with Operations personnel looking over their shoulder!

- And converted it to

  …an interface that many users can access without any supervision, even from a commuter train!



"I'm a very special,
User Friendly GUI,
PC based but Networked
System Management Platform"

Note: Project Notes and Research White Paper is Available.

HMC – Fantastic yes, Secure?

Recommended Best Practices?

We Reference the Following:

- *IBM System z Hardware Management Console Security White Paper*

- *Securing the Hardware Management Console*

www.ibm.com/developerworks/aix/library/au-securinghmc.html
Feb 6, 2007 – The HMC, which plays a central role in the IBM virtualization ... one on the HMC, and he co-authored the HMC Best Practices white paper last year. ... tool to help you secure the Hardware Management Console (HMC).IBM HMC Connectivity Security for IBM POWER5, POWER6 and ...

- *IBM HMC Best Practices*

www-304.ibm.com/webapp/set2/sas/f/best/hmc_best_practices.pdf
File Format: PDF/Adobe Acrobat - Quick View4.8 Managing and Understanding Security Vulnerabilities on HMC ..... 21. 4.9 Resource Monitoring and ..... of this white paper. For the vast majority of HMC

Complementary SHARE Sessions

Complementary Sessions…

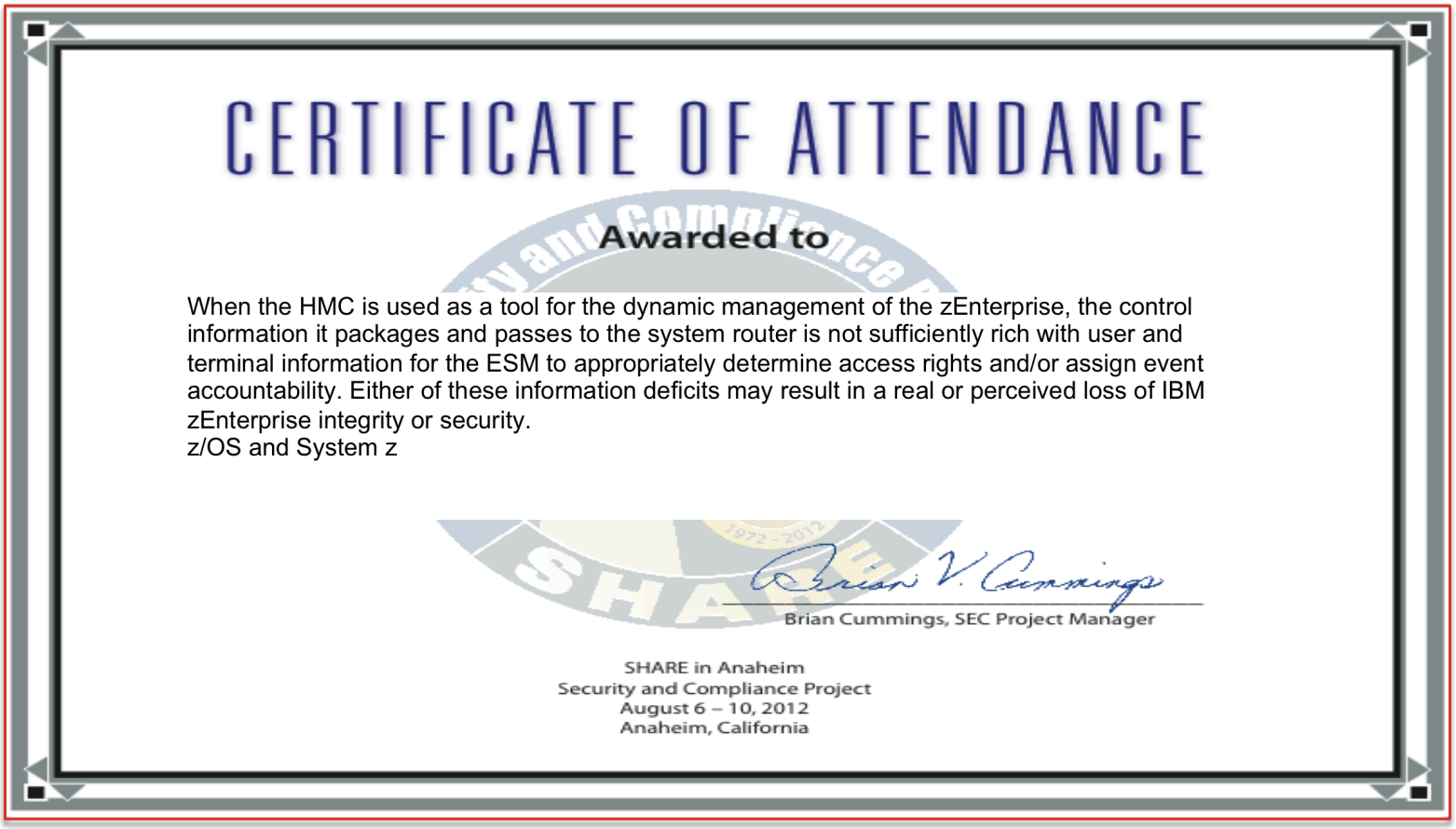
Session 12744: Configuring Health Checker for z/OS – Hands-on Lab
Tuesday, February 5 - 11:00 AM
Union Square 23-24

Session 12255: The HMC (Hardware Management Console) is a Fantastic Feature of the zEnterprise but What Mistakes Are You Making Securing It?
Tuesday, February 5 - 12:15 PM -Plaza B

Session 12807: HMC Security Basics and Best Practices
Tuesday, February 5 - 3:00 PM
Franciscan D

Session 12257: How to Detect Attempted Mainframe Intrusions
Wednesday, February 6, 2013: 3:00 PM
Grand Ballroom B

Continuing Education Credit



CERTIFICATE OF ATTENDANCE

Awarded to

When the HMC is used as a tool for the dynamic management of the zEnterprise, the control information it packages and passes to the system router is not sufficiently rich with user and terminal information for the ESM to appropriately determine access rights and/or assign event accountability. Either of these information deficits may result in a real or perceived loss of IBM zEnterprise integrity or security.
z/OS and System z

Brian Cummings, SEC Project Manager

SHARE in Anaheim
Security and Compliance Project
August 6 – 10, 2012
Anaheim, California

A Statement of Requirements

HMC Security Vs. zEnterprise Integrity and Security

- It is a common z/OS Security best practice to seek full accountability; user, terminal and action identification of events that are intended to modify the functional configuration - the hardware and software of the IBM zEnterprise.
- Functional control over resource access and resource use is provided by the External Security Managers (RACF, CA ACF2, CA Top Secret) and is dependent on this vital information in maintaining the integrity of the IBM zEnterprise environment.
- When the HMC is used as a tool for the dynamic management of the zEnterprise, the control information it packages and passes to the system is not sufficiently rich with user and terminal information for the ESM an appropriately determine access rights and/or assign event accountability.
- This information deficit results in a loss of zEnterprise system integrity and security from the perspective of the External Security Manager and the Security Professionals that depend on it oversight and reporting.

That's it folks, all done!

Session Evaluation – Session Number - 12255

The HMC Is a Fantastic Tool But Are You Making it Secure?

Barry Schrager
Xbridge Systems, Inc.
BSchrager@xbridgesystems.com

Paul R. Robichaux
NewEra Software, Inc.
prr@newera.com

SHARE.org/SanFrancisoEval

Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project

Insert Custom Session QR if Desired.