SEC Project Kickoff - Session 16972

Recent z/OS Security Enhancements

Monday, March 2, 2015: 10:00 AM - 11:00 AM
Sheraton Seattle, Aspen

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

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

Welcome to Seattle - SHARE 60 Years

- **Seattle is the birthplace of Starbucks, the world's largest coffee chain.** You can buy a unique mug (if you collect them) at the original Starbucks in Pike Place Market, first opened in 1971
- **When the Space Needle was built in 1962 for the Seattle World's Fair,** it was the tallest building west of the Mississippi River
- **The bridge that connects Seattle and Medina** across Lake Washington is t**he world's longest floating bridge**
- **Seattle is home to the world's first gas station,** opened on East Marginal Way in 1907
- **Pike Place Market features the longest continuously operating farmer's market in the US**
- **Also home to Boeing and Microsoft (Bill Gates)**

Welcome to Seattle - SHARE 60 Years

Security session highlights:

- Tuesday Keynote is Security Focused – “Soldier of Fortran”
- Wednesday Expert Panel Discussion
- Sessions throughout the week on integrity, protection - Hands-on-Labs, technical sessions on product usage and customer use cases

Join us for Dinner on Wednesday night!

- Place TBD – meet in Sheraton Lobby @ 7pm
- Please let an SEC ribbon wearer know if interested or text our Project Manager @ 412.260.6636 with your name and number of attendees.

Vendor Sponsored Lunch & Learn sessions & Please visit the Expo!

- **C**heck the program guide and message boards by registration.

SHARE

Security and Compliance Project
Session List

SHARE
Educate · Network · Influence

Tuesday Keynote
8:30 AM
The Security Gap
Philip Young
Soldier of Fortran

Wednesday, March 4
7:00 PM
16598 Security & Compliance (SEC)
Project Dinner
Sheraton Lobby


CERTIFICATE OF ATTENDANCE

Awarded to

as presented at the following
Continuing Education Course

Eligible for Continuing Professional Education Credit of One Hour

Carla A. Flores

Carla A. Flores, SEC Project Manager

SHARE in Seattle 2015

Abstract and Speaker

- Upgrading to the latest release of an Operating System is the single most important action that can be taken to assure the integrity of related information systems; their applications and data. In September, 2013 IBM made Version 2 Release 1 of the z/OS Operating System generally available. Are you there yet? Since then a number of APARS have been released to address discovered weaknesses in overall zSystem Security. Are you aware of them?

- In this presentation the focus will be on certain (not all) changes and enhancements to System z Security and the Security of z/OS, its Subsystems and System Management Tools including:

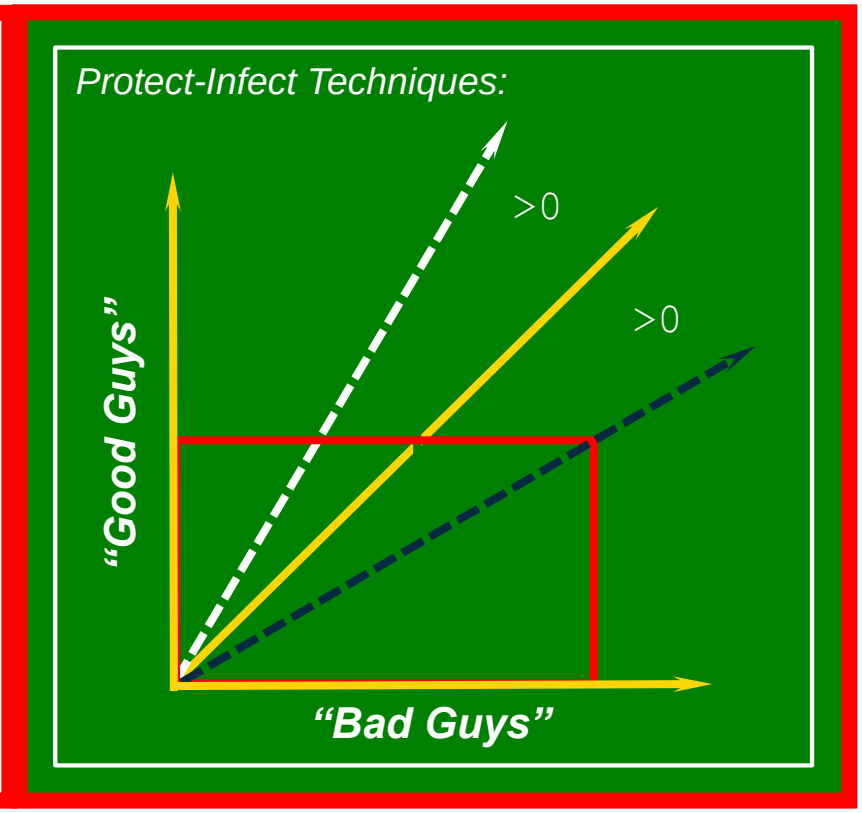
- System z Security Portal
- Security Server RACF
- Operator Commands
- Communication Server
- CICS
- HCD/HCM and, of course, the HMC
- TCP/IP
- ParmLib
- z/OSMF

- Paul R. Robichaux is CEO of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his co-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.

- The corporate mission of NewEra Software is to provide software solutions that help users avoid non-compliance, make needed corrections and in doing so, continuously improve z/OS integrity.

Recent z/OS Security Enhancements

Secure is when "Bad Guys" have a Negligible Advantage!

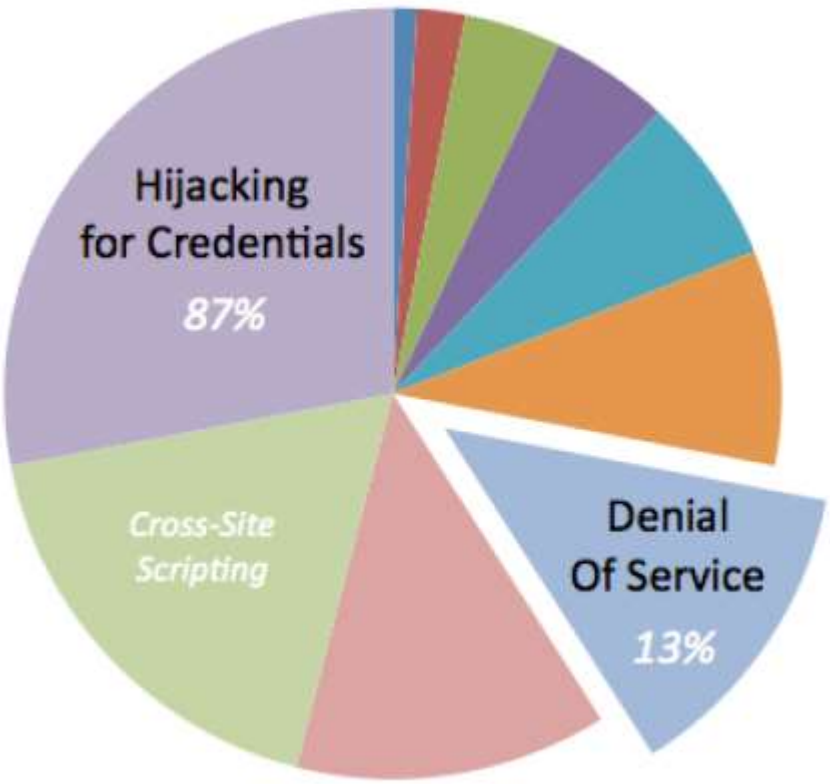


The Goal is to Reduce an Adversary's Advantage to "Zero"!

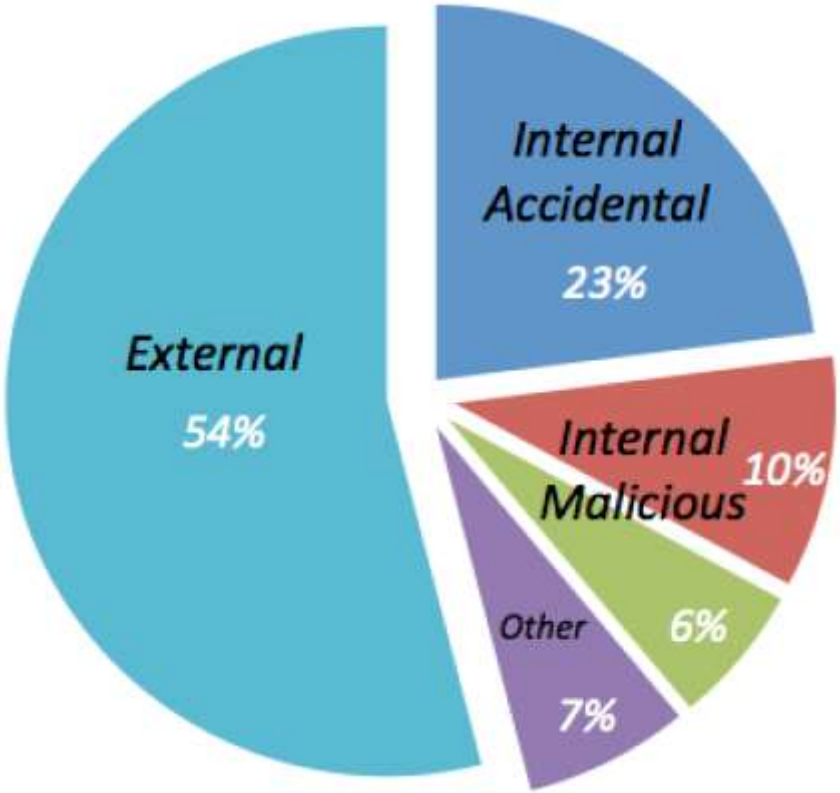
http://en.wikipedia.org/wiki/Advantage_(cryptography)

Recent z/OS Security Enhancements

The "Bad Guys" will use every "Trick in the Book"!



From the Outside



From the Inside

Recent z/OS Security Enhancements

Globally 2015 - Computer Crime Cost Vs. Defense Expense!

$900 Billion +/-

"Bad Guys"

You set it, right?

$75B +/-

"Good Guys"

Something is Wrong!

McAfee 2014 Cost Estimate X 1.5 and Gartner 2015 Defense Projection

Recent z/OS Security Enhancements

Is the System z Mainframe a likely Hacker's Target/Prize?

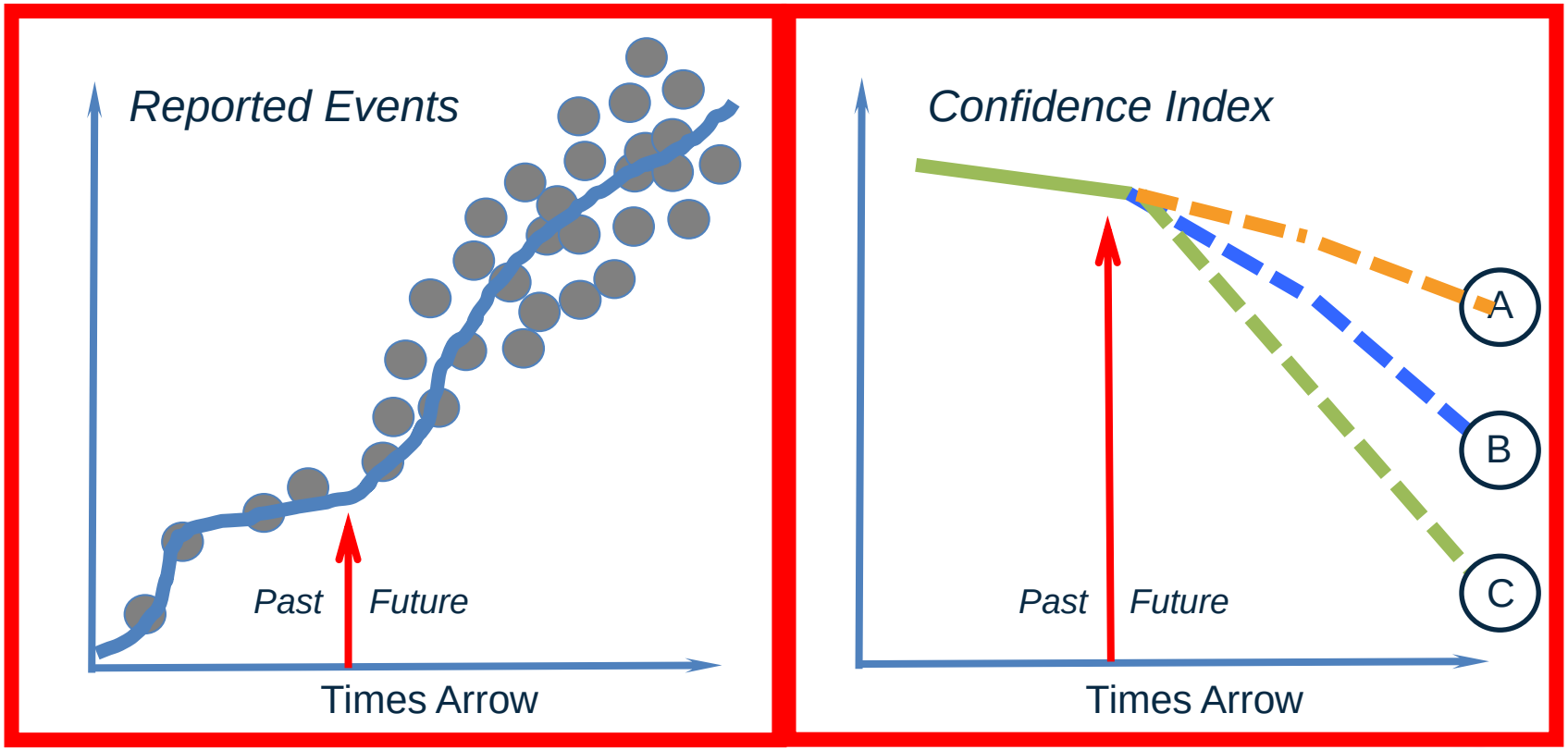
Polismyndigheten
i Stockholms län

[Pirate Bay co-founder charged with hacking IBM mainframes]
[The Hack Details]

[Made available from Phil Young's Tumblr Page]

Recent z/OS Security Enhancements

Connect the Dots - Can you spot and name these trends?



Is there a Tipping Point? See, Malcolm Gadwell

Recent z/OS Security Enhancements

ESM can no longer do it alone! More needs to be done!

External Security Manager (ESM) *Role Based Access Controls*

Perimeter Configuration Boundary *Configuration - Micro Boundary*

System z Configuration Security-Control Continuum

Recent z/OS Security Enhancements

The External Security Manager (ESM)

- What's New in CA-ACF2
- What's New in CA-Top Secret
- What's New in IBM-RACF

"These are Links"

Supplemental Security Manager (SSM)

- Vanguard Integrity Professionals
- Tivoli zSecure Security Suite
- Professional Service Organizations

"These are Links"

Recent z/OS Security Enhancements

System z Security Portal:

IBM Systems > Mainframe servers > Advantages >

Security

Overview | Integrity | Solutions | Resources

Overview | z/OS | z/VM | z/VSE | **Subscription Process**

If you are a System z customer (or their authorized representative), follow the steps described on this page to obtain access to the System z Security Portal for System z Security/Integrity APAR information (currently z/OS and z/VM).

The System z Security Portal is intended to help you stay current with security and system integrity fixes by providing current patch data and now also provides Associated Common Vulnerability Scoring System (CVSS) V2 ratings for new APARs.

To obtain access to the System z Security Portal, send us an email by pressing the following button and provide the customer name, your name and Resource Link ID

Portal Registration

IBM will then verify that you are a System z customer or their authorized representative.

By accessing the System z Security Portal you agree the information contained in it is IBM Confidential, provided AS IS, may be used by you for internal purposes only and may not be disclosed to any third party without IBM's prior written consent.

If you do not agree to these conditions, you may not access the System z Security Portal.

Contact IBM

Chat now
Email IBM
→ Find a Business Partner
Call IBM: 1-866-883-8901
Priority code: 101AS13W

Browse System z

Hardware | Solutions
Software | Operating systems

→ Advantages | → News
→ Community | → New to System z
→ Education | → Resources
→ Literature | → Success Stories
→ Migrate to System z | → Support & services

http://www-03.ibm.com/systems/z/advantages/security/integrity_sub.html

http://www.vm.ibm.com/devpages../SPERA/aparint.html

Recent z/OS Security Enhancements

System z Security Portal:

A Standardized, Free, Common Vulnerability Scoring System (CVSS)

- ☑ Provides an open framework for communicating the characteristics and impact of IT vulnerabilities. CVSS consists of 3 groups:
  - *The Base group represents the intrinsic qualities of a vulnerability.*
  - *The Temporal group reflects the characteristics of a vulnerability that change over time.*
  - *The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment.*
- ☑ From each Group the following is produced:
  - *A numeric score ranging from 0 to 10, and*
  - *A Vector, a compressed textual representation that reflects the values used to derive the score.*
- ☑ This scoring process enables IT managers to more productively evaluate, recognize, prioritize and resolve System Threats across the entire organization.

FIRST = Forum of Incident Response and Security Teams

http://www.first.org/cvss *and* http://en.wikipedia.org/wiki/CVSS

Recent z/OS Security Enhancements

How Secure are your System Access Credentials?

☑ User Password Concerns

- *The 626,718 passwords were harvested during penetration tests over the last two years conducted across corporate America by Trustwave infosec geeks.*

- *The firm's threat intelligence manager Karl Sigler said in a post that half of the plundered passwords were cracked within "the first few minutes".*

Character Types & Combinations	Count	%
Lowercase + Number	212158	36.799%
Lowercase + Uppercase + Number	201447	34.941%
Number Only	72425	12.562%
Uppercase + Lowercase + Number + Special	36386	6.310%
Number + Special	24354	4.224%
Lower Only	12205	2.117%
Uppercase + Number	7306	1.267%
Lowercase + Number + Special	3966	0.688%
Lowercase + Uppercase + Special	3068	0.532%
Uppercase + Number + Special	1309	0.227%
Lowercase + Uppercase	959	0.166%
Uppercase + Special	407	0.071%

"Cracked half in a few minutes. Almost 92 percent of the total sample within a period of 31 days."

https://www.trustwave.com/home/

Recent z/OS Security Enhancements

System z Passwords are RACF Strong!

SETROPTS PASSWORD(HISTORY(number) | NOHISTORY)

SETROPTS PASSWORD(INTERVAL(maximum))

SETROPTS PASSWORD(MINCHANGE(minimum))

SETROPTS PASSWORD(MIXEDCASE | NOMIXEDCASE)

SETROPTS PASSWORD(REVOKE(attempts) | NOREVOKE)

SETROPTS PASSWORD(RULEn(LENGTH(m1:m2) content(position))

SETROPTS PASSWORD(NORULEn | NORULES)

SETROPTS PASSWORD(ALGORITHM(KDFAES) | NOALGORITHM)

SETROPTS PASSWORD(WARNING(days-before) | NOWARNING)

SETROPTS INACTIVE(days-inactive) | NOINACTIVE

Recent z/OS Security Enhancements

APAR OA43999 – RACF password enhancements - 11/2014

Stronger encryption for passwords and password phrases.
SETROPTS PASSWORD(ALGORITHM(KDFAES))
SETROPTS PASSWORD(NOALGORITHM)

Support for 14 additional special characters in passwords.
SETROPTS PASSWORD(SPECIALCHARS)
SETROPTS PASSWORD(NOSPECIALCHARS)

#,$,@. If SPECIALCHARS is in effect, add: .,<,+,|,&,!,*,-,%,_,>,?,:,=
If MIXEDCASE add: a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z

---

Password syntax control that requires a password to contain at least one character from each of four different categories
SETROPTS PASSWORD(RULE1(LENGTH(8) MIXEDALL(1:8)))

LENGTH(1:8) xxxxxxxx - Can a RACF password get stronger than this?

Users to have a password phrase without a password
ALTUSER *userId NOPASSWORD*

- A - Alphabetic
- C - Consonant
- c - Mixed consonant
- L - Alphanumeric
- m - Mixed numeric
- N - Numeric
- V - Vowel
- v - Mixed vowel
- W - Non-vowel
- * - Any character
- $ - National
- s – Special char.
- x – Mixed all

LENGTH(1:8) xxs***xx

ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/oa43999.pdf

Recent z/OS Security Enhancements

A word to the wise. Never forget the following:

If multiple rules are defined, a password that passes at least one rule is accepted.

```
RULE1 LENGTH(1:8) xxs***xx
RULE2 LENGTH(5:8) ********
RULE3 LENGTH(7:8) LLLssLLL
```

The Visualization of Symbols
Used to Define the Format
of RACF Passwords

by

Richard K. Faulhaber

Recent z/OS Security Enhancements

APAR OA43999 – RACF Health Checks Added - 11/2014

RACF_ENCRYPTION_ALGORITHM
SETROPTS PASSWORD(ALGORITHM(KDFAES) | NOALGORITHM)
Reports on the encryption method used for password protection. Exception reported when any method (masking/application) other than DES is used for password protection.

RACF_PASSWORD_CONTROLS
Reports exceptions to the following password rules:

1 - Mixed-case passwords not enabled. Necessary to extend the size of the key space.
SETROPTS PASSWORD(MIXEDCASE | NOMIXEDCASE)
Password syntax rules must be modified to allow mixed case and lower case characters.

2 - Invalid password revocation count is greater than three (3).
SETROPTS PASSWORD(REVOKE | NOREVOKE(*number-of-unsuccessful-attempts)*)
Will revoke the user ID on the next unsuccessful attempt

3 - Maximum number of days a user's password/passphrase is valid is less than 90 days.
SETROPTS PASSWORD(INTERVAL(*maximum-change-interval)*)
The initial supplied default period at RACF initialization is 30 days**??????**

ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/oa45608.pdf

Recent z/OS Security Enhancements

RACF Health Checks - Will more may be coming?

SETROPTS PASSWORD(HISTORY(number) | NOHISTORY)

SETROPTS PASSWORD(INTERVAL(maximum))

SETROPTS PASSWORD(MINCHANGE(minimum))

SETROPTS PASSWORD(MIXEDCASE | NOMIXEDCASE)

SETROPTS PASSWORD(REVOKE(attempts) | NOREVOKE)

→ SETROPTS PASSWORD(RULEn(LENGTH(m1:m2) content(position))

SETROPTS PASSWORD(NORULEn | NORULES)

SETROPTS PASSWORD(ALGORITHM(KDFAES) | NOALGORITHM)

SETROPTS PASSWORD(WARNING(days-before) | NOWARNING)

SETROPTS INACTIVE(days-inactive) | NOINACTIVE

Recent z/OS Security Enhancements

RACF Health Checks - One Check to Rule them All?

ADDCREATOR | NOADDCREATOR
ADSP | NOADSP
APPLAUDIT | NOAPPLAUDIT
AT | ONLYAT([node].userid)
AUDIT | NOAUDIT (class-name)
CATDSNS (FAIL | WARN) | NOCAT
CLASSACT | NOCLASSACT} (class-name)
CMDVIOL | NOCMDVIOL
COMPATMODE | NOCOMPATMODE
EGN | NOEGN
ERASE(ALL|SECLEVEL | NOSECLEVEL | NOERASE
GENCMD | NOGENCMD (class-name)
GENERIC | NOGENERIC (class-name)
GENERICOWNER | NOGENERICOWNER
GENLIST | NOGENLIST (class-name)
GLOBAL | NOGLOBAl (class-name)
GRPLIST | NOGRPLIST
INACTIVE(unused-userid-interval) | NOINACTIVE
INITSTATS | NOINITSTATS
BATCHALLRACF | NOBATCHALLRACF
EARLYVERIFY | NOEARLYVERIFY
XBMALLRACF | NOXBMALLRACF
NJEUSERID(userid)
UNDEFINEDUSER(userid)
KERBLVL(0|1)
LANGUAGE(PRIMARY) or (SECONDARY)
LOGOPTIONS(ALWAYS(class-name)
LOGOPTIONS(NEVER(class-name)
LOGOPTIONS(SUCCESSES(class-name)
LOGOPTIONS(FAILURES(class-name)
LOGOPTIONS(DEFAULT({class-name)
MLACTIVE [(FAILURES | WARNING)] | NOMLACTIVE]
MLFSOBJ (ACTIVE | INACTIVE)
MLIPCOBJ (ACTIVE | INACTIVE)
MLNAMES | NOMLNAMES
MLQUIET | NOMLQUIET
MLS [(FAILURES | WARNING)] | NOMLS
MLSTABLE | NOMLSTABLE
MODEL(GDG | NOGDG)
MODEL(GROUP | NOGROUP)
MODEL(USER | NOUSER)
NOMODEL
OPERAUDIT | NOOPERAUDIT
PASSWORD(HISTORY(number) | NOHISTORY))
PASSWORD(INTERVAL(maximum))
PASSWORD(MINCHANGE(minimum))
PASSWORD(MIXEDCASE | NOMIXEDCASE))
PASSWORD(REVOKE(attempts) | NOREVOKE))
PASSWORD(RULEn(LENGTH(m1:m2) content(position))
PASSWORD(NORULEn)
PASSWORD(NORULES)
PASSWORD(WARNING(days-before) | NOWARNING))
PREFIX(prefix) | NOPREFIX
PROTECTALL [(FAILURES | WARNING)] | NOPROTECTALL
RACLIST | NORACLIST} (class-name)
REALDSN | NOREALDSN
RETPD(nnnnn)
RVARYPW([SWITCH(switch-pw)] [STATUS(status-pw)])
SAUDIT | NOSAUDIT
SECLABELAUDIT | NOSECLABELAUDIT
SECLABELCONTROL | NOSECLABELCONTROL
SECLBYSYSTEM | NOSECLBYSYSTEM]
SECLEVELAUDIT (security-level) | NOSECLEVELAUDIT
SESSIONINTERVAL(n) | NOSESSIONINTERVAL
STATISTICS | NOSTATISTICS} ({class-name)
TAPEDSN | NOTAPEDSN
TERMINAL(NONE | READ)
WHEN | NOWHEN} (PROGRAM)

Risk Management Framework (RMF) for DoD IT - NIST z/OS RACF STIG v6r21

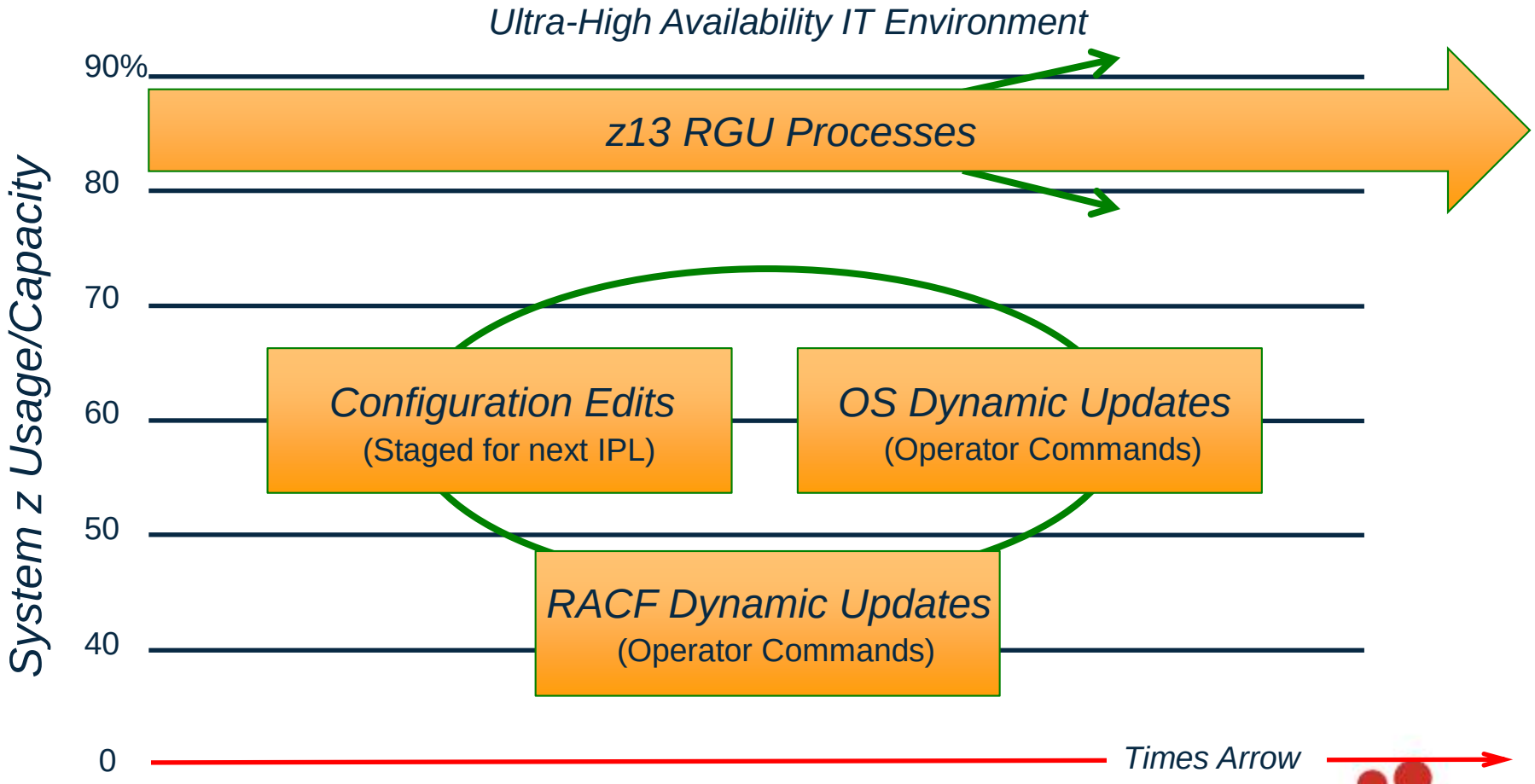
Recent z/OS Security Enhancements

RACF Updates in V2R1

- RRSF (RACF Remote Sharing Facility - now using TCP/IP instead of APPC)
  - Support for TCP/IP V6 (extending the existing IPV4 Support)
  - Comments in the RACF parameter library
  - TLS 1.2 cipher suite support
- New and improved RACF Health Checks
  - RACF_AIM_STAGE
  - RACF_UNIX_ID
  - RACF_CERTIFICATE_EXPIRATION
  - RACF_SENSITIVE_RESOURCES
- In IRRDBU00 output
  - Certificate issuer distinguished name
  - Subject distinguished names
  - Signature algorithms
- &RACUID in home directory path name
- Access controls for JES2/JES3 job classes

Recent z/OS Security Enhancements

Dynamic Updates - More Agile but Compliance is Difficult!



Recent z/OS Security Enhancements

Operator SET Commands - More Dynamic and More Agile!

Command	Authority	Resource-Name
SET CON	UPDATE	MVS.SET.CON
SET GTZ	UPDATE	MVS.SETGTZ.GTZ
SETALLOC	UPDATE	MVS.SETALLOC.ALLOC
SETIOS	UPDATE	MVS.SETIOS.IOS
SETHS	UPDATE	MVS.SETHS
SETLOAD	UPDATE	MVS.SETLOAD.IEASYM/LOAD
SETLOGR	UPDATE	MVS.SETLOGR.LOGR
SETOMVS	UPDATE	MVS.SETOMVS.OMVS
SETPROG	UPDATE	MVS.SETPROG
SETSMS	UPDATE	MVS.SETSMS.SMS
SETUNI	UPDATE	MVS.SETUNI.UNI

*Class M1 and M2 commands attach and run in the *MASTER* address space.*

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Recent z/OS Security Enhancements

Operator SET Commands - More Dynamic and More Agile!

- SET CON - *enables you to add MCS consoles dynamically when they are being used in distributed mode. It processes a CONSOLxx parmlib member and adds new consoles, up to the system and sysplex limits for the maximum number of consoles.*

SET [CON={(xx,[xx]...)}]

Where xx is the suffix of the target CONSOLxx parmlib member.

- SETCON - *enables you to specify a console to be removed from the sysplex and/or system. All resources associated with the named console will be freed and/or removed.*

SETCON {DELETE,CN=nnnnnnnn}

Where nnnnnnnn is the Console Name.

Note: The system pins UCBs for console devices defined in CONSOLxx at IPL time. Deleting a console device using HCD requires an IPL unless IEARELCN was used; a version of this program is found in SYS1.SAMPLIB.

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Recent z/OS Security Enhancements

Operator SET Commands - More Dynamic and More Agile!

☑ AUTHSETSMF | NOAUTHSETSMF - Specifies whether changes are authorized to be made to the SMF parameter options via the SETSMF command.

☑ The SETSMF command is not authorized under either of the following conditions:

- The NOAUTHSETSMF SMFPRMxx parmlib option is specified.
- The PROMPT(IPLR) or NOPROMPT SMFPRMxx parmlib options are specified, and the AUTHSETSMF parmlib option is NOT specified.

☑ The SETSMF command is authorized under either of the following conditions:

- The AUTHSETSMF SMFPRMxx parmlib option is specified.
- The PROMPT(LIST) or PROMPT(ALL) SMFPRMxx parmlib options are specified.

APAR: If SMF is set to a parmlib member that contains the NOPROMPT or PROMPT(IPLR) option as well as the AUTHSETSMF option, subsequent changes to the SMF configuration via the SETSMF command are honored. In this case, if SMF is then set to a parmlib member that contains NOPROMPT or PROMPT(IPLR) but does not contain the AUTHSETSMF option, SETSMF configuration changes are erroneously honored. This is because the internal indicator for the AUTHSETSMF option is not cleared for subsequent SETs when the option is not specified.

Recent z/OS Security Enhancements

Operator SET Commands - More Dynamic and More Agile!

- SETLOAD - *supports updating the values of system symbols dynamically. A new Keyword enables you to specify that the values of local static system symbols be updated using the values from an IEASYMxx member of parmlib.*

SETLOAD xx,{PARMLIB|IEASYM

Where xx is the suffix of the target LOADxx iplparm member.

- SETPROG - *Hardware Instrumentation Services (HIS) collects hardware event data in SMF records type 113, subtypes 1 and 2, and/or some z/OS UNIX files. Use the sub-command TRACKDIRLOAD to enable system-wide tracking of directed load modules.*

SETPROG TRACKDIRLOAD|NOTRACKDIRLOAD

Note: A directed load module is one loaded to a specified storage address. When enabled, mapping information about directed load modules is included in the maps produced by HIS. Tracking ENABLED by default.

Recent z/OS Security Enhancements

Other Operator Commands - More Dynamic and More Agile!

Command	Authority	Resource-Name
MODIFY	UPDATE	MVS.MODIFY.JOB/STC
SLIP	UPDATE	MVS.SLIP
START	UPDATE	MVS.START.STC.xxxxxxxx
VARY CN	UPDATE	MVS.VARY.CN
CONTROL V	READ[1]	MVS.CONTROL

[1] *The access authority for all CONTROL commands is normally READ, but the L=name (console name) operand can change the access level. When L=name specifies a console that is not full-capability and is not the issuing console, the access authority is UPDATE. When L=name specifies a console that is full-capability and is not the issuing console, the access authority is CONTROL.*

CONTROL V has sysplex scope only when *L=console_name* is specified.

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Recent z/OS Security Enhancements

Other Operator Commands - More Dynamic and More Agile!

- CONTROL V,LOGON|LOGOFF - *supports updating of system control functions that require a System Operator to log on and/or log off of MCS, SMCS, and HMCS Consoles, overriding settings defined in the CONSOLxx member of parmlib.*

- The CONSOLE statement in the CONSOLxx parmlib member establishes a device as an MCS, HMCS or SMCS console and defines its attributes.

```
CONSOLE LOGON {(REQUIRED)} Logon before issuing commands
              {(OPTIONAL)} Always optional for the System Console
                 {(AUTO) } Logged on using Console Name as UserId

DEFAULT LOGON {(REQUIRED)} These are System-Wide Defaults that
              {(OPTIONAL)} apply to all Consoles without specific
                 {(AUTO) } Log on/Log off specifications.
```

- Best Practice - Configure such that SMCS consoles are LOGON(REQUIRED), either by the system-wide DEFAULT or by the individual CONSOLE statement.

The system console is always treated as LOGON(OPTIONAL).

Recent z/OS Security Enhancements

Operator Display Commands - More Information Available!

Command	Authority	Command Description
D CONSOLE	READ	Console status information
D GRS	READ	Global resource serialization information
D GTZ	READ	Generic Tracker Information
D HIS	READ	Hardware event data collection status
D HS	READ	Basic HyperSwap Information
D LIST|ALL	READ	System activity
D OMVS	READ	z/OS UNIX System Services Status
D PCIE	READ	PCIe information
D PPT	READ	PPT information
D PROG	READ	Status of PROG, TRACKDIRLOAD option
D SLIP	READ	SLIP Trap information
D VIRTSTOR	xxxx	Virtual Storage Information
D XCF	READ	XCF information

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Recent z/OS Security Enhancements

Display PPT - IBM Program Properties Table:

PgmName	NC	NS	PR	ST	ND	BP	Key	2P	1P	NP	NH	CP
AHLGTF	Y	Y	.	Y	.	.	0	.	.	Y	.	.
AKPCSIEP	.	Y	.	Y	Y	.	1	.	.	Y	.	.
ANFFIEP	.	Y	.	Y	Y	.	1	.	.	.	.	.
APSHPOSE	.	Y	.	Y	Y	.	1	.	.	Y	.	.
APSKAFPD	.	Y	.	Y	Y	.	1	.	.	Y	.	.

Synonym	----------Meaning----------	----SCHEDxx keyword-----
NC	Non-cancelable	NOCANCEL
NS	Non-swappable	NOSWAP
PR	Privileged	PRIV
ST	System task	SYST
ND	No dataset integrity	NODSI
BP	Bypass password protection	NOPASS
Key	PSW key for this program	KEY(x)
2P	Second level preferred storage	SPREF
1P	First level preferred storage	LPREF
NP	No preferred storage	NOPREF
NH	No honor IEFUSI region settings	NOHONORIEFUSIREGION
CP	Critical paging	CRITICALPAGING

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Recent z/OS Security Enhancements

IBM Program Properties Table - SYS1.LINKLIB(IEFSDPPT)

Table 34. IBM-supplied Program Properties Table (PPT) Values

Program Name	Program Description	NC	NS	PR	ST	ND	BP	Key	2P	1P	NP	NH	CP
AHLGTF	GTF	x	x		x			0			x		
AKPCSIEP	ISP		x		x	x		1			x		
ANFFIEP	IP Printway		x		x	x		1					
APSHPOSE	PSF AFP Download Plus		x		x	x		1			x		
APSKAFPD	PSF Download		x		x	x		1			x		
APSPPIEP	PSF		x		x	x		1			x		
ASBSCHIN	APPC/MVS Scheduler Address Space (ASCH)		x		x			1	x	x			
ASBSCHWL	APPC/MVS Message Log Writer			x				1					
ATBINITM	APPC/MVS Address Space		x		x			1	x	x			
ATBSDFMU	APPC/MVS SDFM Utility			x				1					
AVFMNBLD	AVM	x	x		x			3			x		

z/OS V2R1.0 MVS Initialization and Tuning Reference, Page 728 - 732

Recent z/OS Security Enhancements

Display PROG TRACKDIRLOAD - For Better SMF Records!

☑ DISPLAY PROG,TRACKDIRLOAD displays the status of the TRACKDIRLOAD option: {IN EFFECT | NOT IN EFFECT}

•Syntax is:

D PROG,TRACKDIRLOAD [,L={a|name|name-a}]
Where L=*a, name, or name-a* Specifies the display area (*a), console name (name), or both (name-a) where the* display is to appear.

- Example:

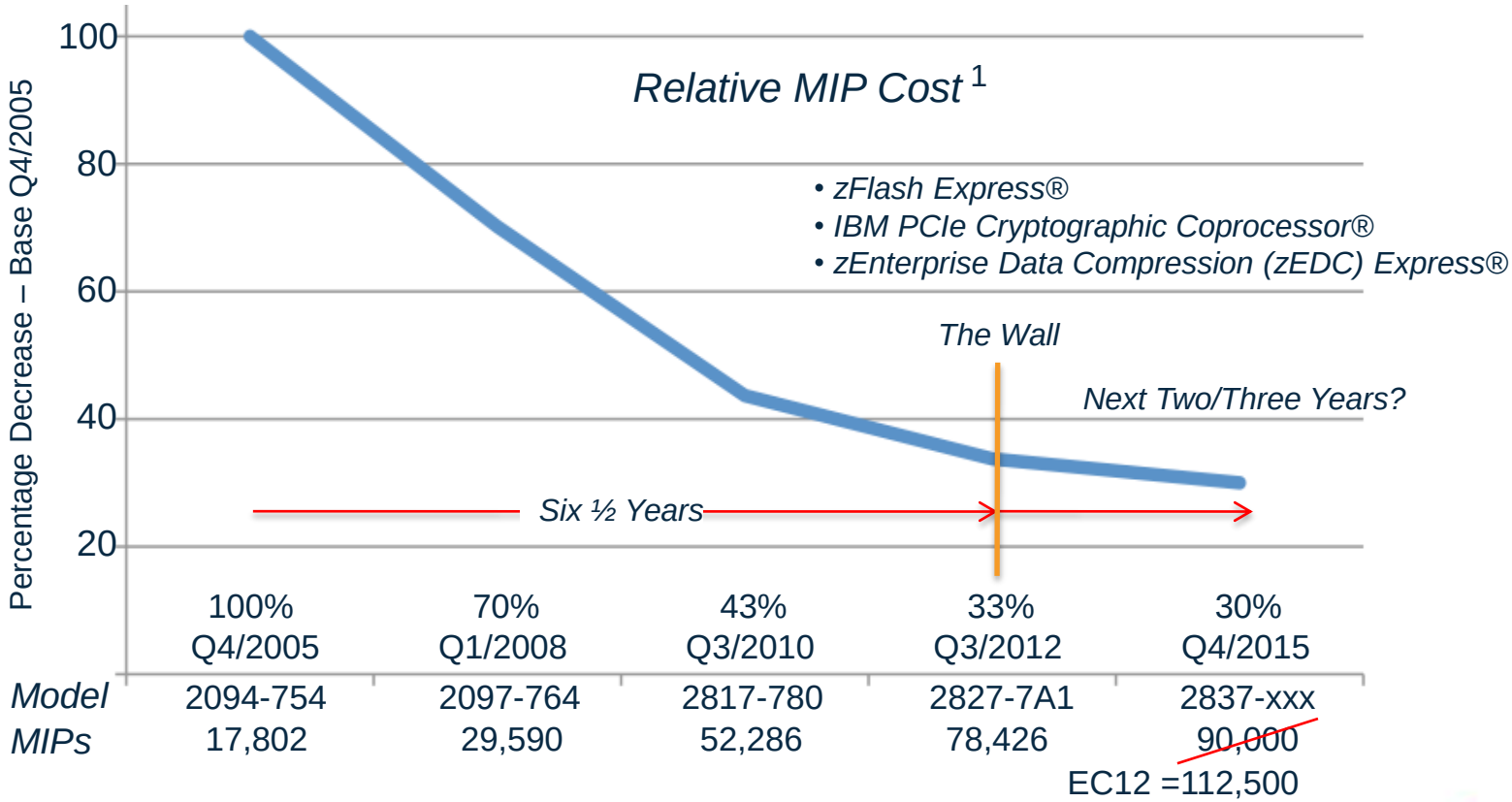
CSV567I TRACKDIRLOAD IS {IN EFFECT | NOT IN EFFECT}

Note: When TRACKDIRLOAD is in EFFECT Hardware Instrumentation Services (HIS) collects hardware event data in SMF records type 113, subtypes 1 and 2, and/or some z/OS UNIX files. Use the sub-command TRACKDIRLOAD to enable system-wide tracking of directed load modules.

z/OS MVS System Commands Version 2, Release 1 SA38-0666-00

Recent z/OS Security Enhancements

Hardware Updates!



[1] Source:http://www.tech-news.com/publib/pl2084.html | pl2094 | pl2097 | pl2817 | pl2827

Recent z/OS Security Enhancements

DMA Attacks

- *A type of side channel attack where the corruption of basic OS security mechanisms or theft of cryptographic keys can be conducted by an attacker with direct access to the physical memory address space of the computer.*
  - Systems are vulnerable to a DMA attack by an external device if they have port like PCI and PCI-Express that can be hooked up directly to a physical address space. Security concerns argue against the use of PCIe as a host-to-host interconnect. See Federal Information Processing Standards - FIPS 140-2 - Levels of Defenses.

- *IQPPRMxx*
  - A z/OS parmlib member whose suffix is specified in IEASYSxx on the IQP Keyword is used to define parameters that manage applications that require the utilization of System z PCIe-related features, such as:
    - *zFlash Express®*
    - *IBM PCIe Cryptographic Coprocessor®*
    - *zEnterprise Data Compression (zEDC) Express®*

PCIe - *Peripheral Component Interconnect*

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Recent z/OS Security Enhancements

IQPPRMxx

☑ ZEDC - *Use the ZEDC statement to specify parameters for managing application requests that use zEnterprise Data Compression (zEDC) features.*

- MAXSEGMENTS - A Keyword
  Specifies the maximum number of 16 MB storage areas (segments) to allow for problem state compression (deflation) and decompression (inflation) requests.
- DEFMINREQSIZE - A Keyword
  Specifies the minimum size in kilobytes of the data to be compressed in order for request to be eligible for zEDC compression.
- INFMINREQSIZE - A Keyword
  Specifies the minimum size in kilobytes of the data to be decompressed in order for the request to be eligible for zEDC decompression.
- SET IQP - An Operator Command
  Used to change the MAXSEGMENTS value to a lower value, the change is ignored and the original value remains in effect, because the maximum number of segments cannot be decreased dynamically. If a higher value is specified, the value is accepted.

z/OS V2R1.0 MVS Initialization and Tuning Reference, Page 591 - 592

Recent z/OS Security Enhancements

TCP/IP

- *What is Remote Direct Memory Access (RDMA)?*

  For security reasons, it is undesirable to allow transmitters to read or write arbitrary memory on the receiver. Any RDMA scheme must prevent any unauthorized memory accesses. Most RDMA schemes protect memory by allowing RDMA reads/writes only to buffers that the receiver has explicitly identified to the NIC as valid RDMA targets. The process of informing the NIC about a buffer is called "registration". The name of a registered buffer is its Region Identifier (RID) - a memory buffer region reserved and registered for use with RDMA requests, and its unique identifier.

- *PORT and/or PORTRANGE STATEMENT*

  Keyword - NOSMCR - Indicates that Shared Memory Communications via Remote Direct Memory Access (SMC-R) communications are not permitted for TCP connections by using a named port and/or any port in a specified range.

RDMA, aka SMC-R - used for direct CPC to CPC Communications.
Like LPAR to LPAR using HyperSockets but for the CPC to CPC over TCP/IP.

z/OS Communications Server: IP Configuration GuideSC27-3650-00

Recent z/OS Security Enhancements

TCP/IP - Profile Configuration

- The PORT statement is used to reserve a port for one/more job names or to control application access to unreserved ports.
- For example, use the PORT statement to control the port that will be used by the SMTP server for receiving mail. If PORT is not coded, SMTP defaults to the value 25, the well known port for mail service.
- Note that port 25 is typically reserved in hlq.PROFILE.TCPIP for the SMTP server to accept incoming mail. If another port number is selected for the SMTP server, then update the hlq.PROFILE.TCPIP file accordingly.

TCP/IP - Port Configuration Statement Syntax

```
>>-PORT----+-num--+-TCP-+--+-RESERVED----------------+-----------------+-+-><
           |        '-UDP-'  '-jobname--+-------------+-'                |
           |                            '-| Options |-'                  |
           |                                            .-WHENLISTEN-.    |
           '-UNRSV--+-TCP--+-jobname--+-------------+-+--+------------+-+-'
                    |       |          '-SAF resname-' |  '-WHENBIND---'  |
                    |       '-*--+-------------+-------'                 |
                    |            +-DENY--------+                         |
                    |            '-SAF resname-'                         |
                    |                                            .-WHENBIND-.
                    '-UDP--+-jobname--+-------------+-+--+----------+---'
                           |          '-SAF resname-' |
                           '-*--+-------------+-------'
                                +-DENY--------+
                                '-SAF resname-'
```

SAF

Source: IBM z/OS V2R1 CS TCP/IP Implementation

z/OS Communications Server: IP Configuration GuideSC27-3650-00

Recent z/OS Security Enhancements

TCP/IP Profile DECK

- *SMFCONFIG STATEMENT (SMC-R Shared Memory Communication)*
  - *SMCR | NOSMCRGROUPStatistics* - Requests, or not, that SMF type 119 records of subtype 41 containing statistics related to SMC-R link groups are created. These records are created periodically based on the SMF interval in effect. This operand is valid if the current record type setting is TYPE119. Default - No Record.
  - *SMCR | NOSMCRLINKEvent* - Requests, or not, that SMF type 119 records of subtype 42 and 43 are created. The SMF records of subtype 42 are created when SMC-R links are started, and the SMF records of subtype 43 are created when SMC-R links are ended. Default - No Record.
- *New command to verify TCP profile syntax*
  - V TCPIP,,SYNTaxcheck,dsname
  - Can run on any system at the same level

Note – TCP/IP Profile DECK, IPSECURITY Keyword on the IPCONFIG Statement
The AUTOLOG Statement, Do you know what it does?

z/OS Communications Server: IP Configuration GuideSC27-3650-00

Recent z/OS Security Enhancements

CICS V5R1

- *RACFSYNC - The system initialization table (SIT) parameter specifies whether CICS listens for type 71 Events.*
  - When CICS receives a type 71 ENF event for a user ID, all cached user tokens for the user ID are invalidated, irrespective of the setting of the USRDELAY parameter. Subsequent requests from that user ID force a full RACF RACROUTE VERIFY request, which results in a refresh of the user's authorization level. User tokens for tasks that are currently running are not affected.
- *SECVFYFREQ* - {NEVER|USRDELAY} *The system initialization table (SIT) parameter specifies whether or not CICS makes a full verification request at least once a day for each user ID that is used to log on to the CICS region.*
  - NEVER - When the login process uses password verification, CICS makes a full verification request only if an attempt at password verification fails.
  - USRDELAY - CICS makes a full verification request at least once a day for each user ID that is used to log on to the CICS region.

Recent z/OS Security Enhancements

Hardware Configuration Definitions - HCD/HCM

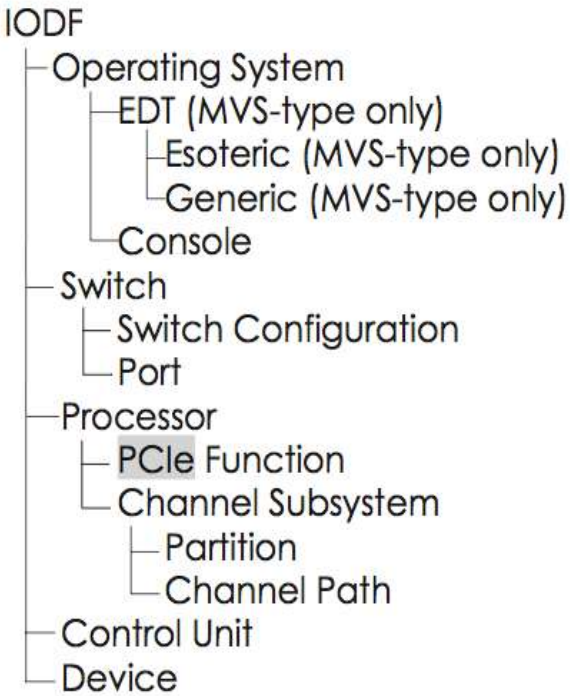
- ☑ PCIe - *Peripheral Component Interconnect Express adapters attached to a 2827 type system can provide the operating system with a variety of so-called PCIe functions to be exploited by entitled logical partitions (LPARs).*

- ☑ HCD - *allows you to define, change, delete, and view PCIe functions controlling which LPARs have access to their functions.*

  - Remote Direct Memory Access (RDMA) over Converged Ethernet (RoCE). PCIe functions of type RoCE may be assigned to external physical networks by specifying corresponding PNET IDs.

  - zEDC-Express. For PCIe functions of type zEDC-Express, a virtual function number between 1 and 15 must be specified.

Structure:



http://publibz.boulder.ibm.com/epubs/pdf/cbd2ug00.pdf

Recent z/OS Security Enhancements

Hardware Configuration Definitions - HCD/HCM

- PCIe - *Specified on IODF FUNCTION Statement*:

```
FUNCTION FID=05A,UNIT=ROCE,PCHID=54A
         PNETID=(PNET01,PNET02,PNET03)
         PART=((LP01,(LP03,LPO8)
         DESC='zEDC Express one'
```

- PCIe - *Activity Report:*
  - Provides statistics and performance measurements on PCI Express based functions (PCIE functions) allocated by at least one z/OS address space for a period of time within the reporting interval.
  - SMF data required for this report is gathered by default. PCIE functions are captured by the report if hardware feature activities have been detected.

Not Defined to any specific LCSS - Logical Channel Subsystem

Syntax:

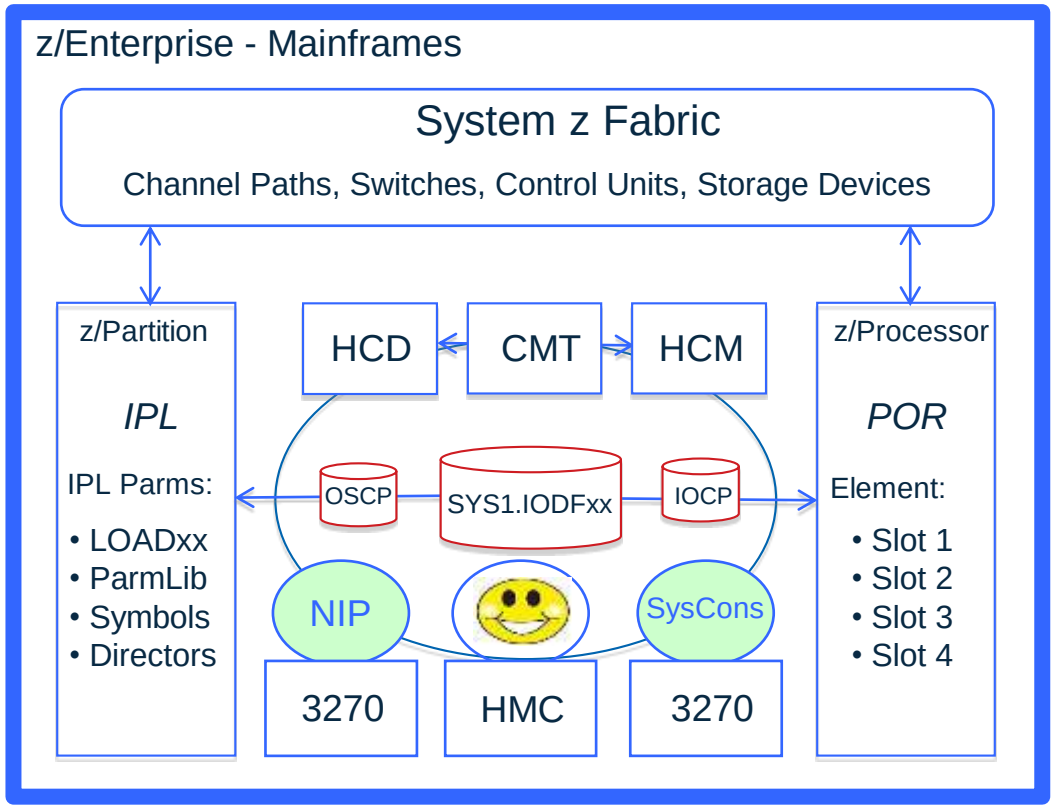
Partition	Name
	Number
	Usage
	Description
PCIe function	ID
	Unit
	PCHID
	Virtual function number
	Description
	PNET IDs
	Partition access list
	Partition candidate list

http://publibz.boulder.ibm.com/epubs/pdf/cbd2ug00.pdf

Recent z/OS Security Enhancements

HMC - Hardware Management Console

- ☑ *You can operate a z/OS system or an entire Sysplex using the Operating System OS Message Facility of the Hardware Management Console (HMC). This can also be known as 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.*



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

Recent z/OS Security Enhancements

HMC - Hardware Management Console

- *The HMCS can be used as a NIP console if attached from the HMC to a z/OS LPAR, that is then IPLed. For "consistency" the HMCS NIPs interface is identical to that of NIP, MCS, SMCS consoles.*
- *If you want to use the HMCS consoles after NIP, you'll need to define it in the CONSOLxx member.*
- *To do this use the CONSOLxx Keyword "HMCS" to defines a new console type that bridges the gap between NIP and SMCS console allowing you to use the HMCS as a console during IPL, and before and after SMCS type consoles become available.*

- *Likely in response to a SHARE Requirement to replace OSA-ICC style consoles previously needed in order to perform similar multi-role functions.*

Attribution for Understanding: Thank you Marna Walle!

Syntax:

```
CONSOLE DEVNUM {(devnum)}
               {(SUBSYSTEM)}
               {(SYSCONS)}
               {(SMCS)}
               {(HMCS)}
```


z/OS V2R1.0 MVS Initialization and Tuning Reference, Page 236 - 247

Recent z/OS Security Enhancements

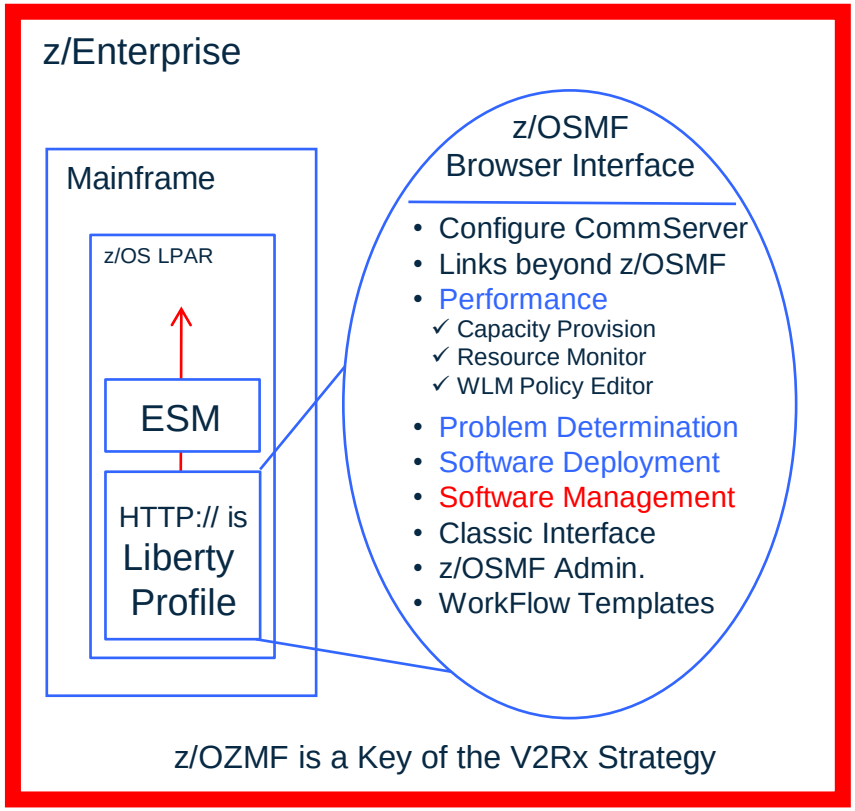
z/OSMF

- ☑ 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.

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.



→ *V2R2 No longer separate - V2R3 z/OSMF will "Always be On".*

IBM z/OS Management Facility Configuration GuideSA38-0657-00

Recent z/OS Security Enhancements

System Management Platforms are Converging!

TSO/ISPF
Classic Interface

z/Manager
Hardware Interface

EKMF Workstation
Enterprise Key Management

z/OSMF
Software Interface

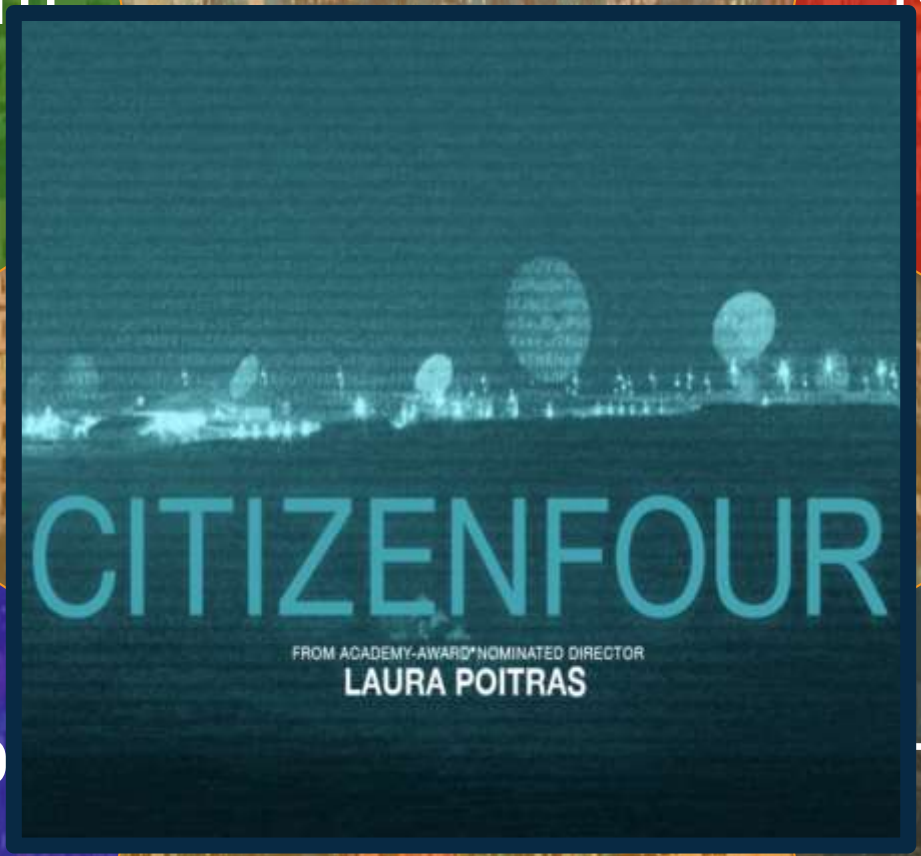
z13

EKMF = Enterprise Key Management Facility


OS/System Team
Net Work Team
Security Team
Application Team
Hardware Team

OS/System Team

Net Work Team



Applicatio Team

Hardware Team

Thank you. Your evaluation please!

SEC Project Kickoff - Session 16972

Recent z/OS Security Enhancements

Monday, March 2, 2015: 10:00 AM - 11:00 AM
Sheraton Seattle, Aspen

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