How Secure is Your Mainframe, Really?

Brian Cummings, Tata Consultancy Services
Mark S Hahn, IBM

Tuesday, March 13, 2012
10902

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

SHARE in Atlanta 2012

Two-Part Presentation

Concerns

Actions

The Mainframe Lives?

The future of the mainframe: A CIO survey by The Standish Group

Posted on 10. May, 2011 by **Micro Focus** in

News, **Research**, **White Papers**

What does the future hold for the mainframe? It's a question that's frequently asked and to provide some answers once and for all the Standish Group recently undertook a survey of CIOs at Fortune 1000 companies about their use of the mainframe.

The survey findings give valuable insight into the perceptions and intentions of the CIOs:

- 70% said that while the mainframe plays a strategic role in their organization today, in five years NONE of the CIOs considered that the mainframe would play a central role
- 59% propose to migrate core mainframe applications to a Windows, UNIX or Linux platform
- 78% are either currently engaged in a modernization exercise or plan to be within 18 months – leaving 22% without a modernization plan.

The Mainframe Lives?

Home > Topics > IT management > IT strategy > Is the time right for a mainframe renaissance?

Is the time right for a mainframe renaissance?

+1 0 Tweet 0

Every few years, industry pundits predict the death of the mainframe. But these big iron systems, represent the IT lifeblood of major enterprises. Far from being killed off, the mainframe is being re-incarnated as a modern system for internet applications, service oriented architectures (SOAs) and enterprise resource planning.

- Plugging the mainframe skills gap
- IBM lowers mainframe costs with specialty processors
- Attracting new mainframe customers

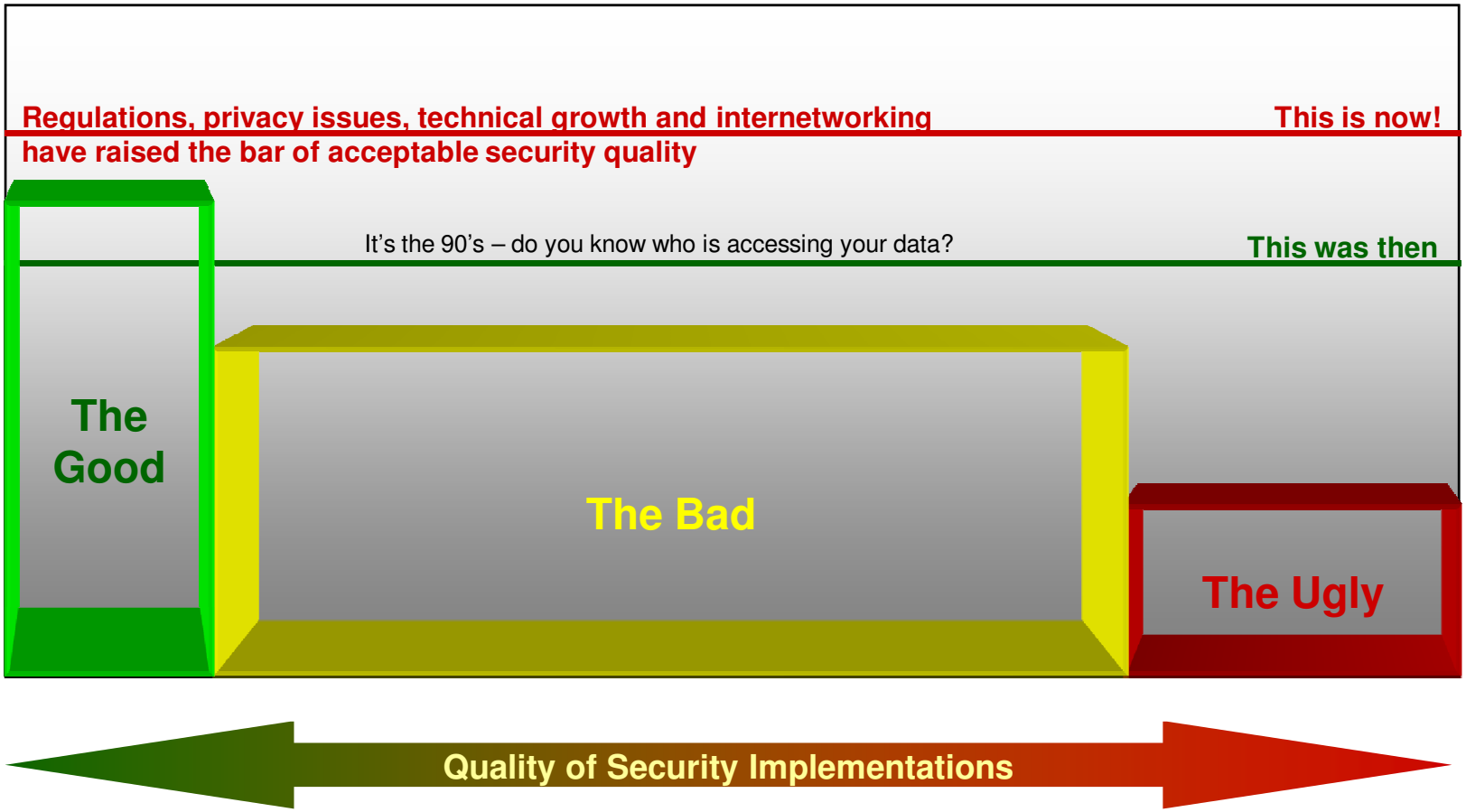
Many people perceive the mainframe as an expensive necessity, required for business-critical systems. Over time, many of these systems have been migrated to PC and Unix servers configured in mutli-tiered distributed architectures, where servers are allocated specific functions to support the business applications and provide high availability. There are, however, hidden costs associated with distributed computing environments, which is driving businesses to re-assess the mainframe as a platform.

According to IBM, an IBM System z10 EC mainframe has the equivalent capacity of nearly 1,500 x86 servers with an 85% smaller footprint and up to 85% lower energy costs. While the starting price of this machine is around the $1 million mark, WinterGreen Research has estimated that seven times more IT administrators are required to run a real time, 24 by 7, high-availability distributed computing environment compared to running the same

Is the Mainframe Vulnerable?

- Hacking/Theft
  - 2007 T J Maxx Breach mainframe security hack
  - 2008 LensCrafters mainframe security hack
  - 2009 Mainframe computer physically stolen from Trinity Valley Community College
  - 2010 Sydney Airport mainframe computer physically stolen
- Insider Threat?
  - Long considered the most serious threat
    - Insiders have access
    - Insiders have knowledge
    - Insiders have economic motivation
    - Insider collusion is a “force multiplier”

Change Can Leave You Behind



Mainframe Vulnerabilities

Mainframe Security Report 1:

Security Officer Representation: We restrictively secure our mainframe based-on the concept of "least privilege". Nobody gets access to anything unless it is approved.

Report Finding: The mainframe security and the protection-by-default mechanisms of the mainframe security software have been promiscuously configured to the point of providing access by default instead of protection. The security of system and application resources cannot be assured.

Reality of security contradicts perception

Mainframe Vulnerabilities

Mainframe Security Report 2:

Security Officer Representation: It is our practice to empower business units to make decisions regarding the security of their applications and services.

Report Finding: As authorized by a business unit, CICS regions were running with full security bypass privilege, leaving CICS technical resources and the data of all applications vulnerable to system programmers, CICS sub-system programmers, and application programmers. Result: No separation of function between applications; no assurance of data privacy protection; no assurance of production operation.

No Security Implementation Standards
a.ka. "Adult Supervision"

Mainframe Vulnerabilities

Mainframe Security Report 3:

Mainframe security is being managed and administered using legacy practices and standards that pre-date the increased technical sophistication of the mainframe and its increased leverage for Web-based services. As such, security is woefully inadequate to assure security , privacy, and compliance in the current environment.

Mainframe is Dead Legacy…

Low investment, weak skills, weak governance, maybe coupled with a false sense that the mainframe is inherently secure

Story of a Security Consultant

Unix System Services Hack

Due to the regular mis-configuration of security in the z Unix System Services environment and inappropriate use of security bypass privileges, one security practitioner has repeatedly demonstrated the ability to compromise mainframe security and grab any data desired.

His record hack time: Less than 20 minutes!!!

One of the successes was by invitation against a security software company.

Story of a Security Consultant

Mainframe Security Penetration Test

A mainframe security penetration test used a basic, low-privilege TSO account.

Using the account, the testers discovered a site-defined Supervisor Call (SVC)

The SVC provided an emergency security bypass account for the system programmer, and the password was incorporated in the source code in plain text.

Result: Complete system compromise

Advice of a Career Auditor

"You don't know what you don't know, and what you don't know will hurt…!"

David Hayes,
U.S. Government Accountability Office

SHARE 2012 Atlanta

SEC Project Keynote Presentation

TCS InfoSec Optimization Principles

Vision

- Strategy, Policy, Standards
- Governance, Organization
- Business Alignment
- Targeted Maturity Level and Roadmap

Visibility

- Information asset identification
- Risk assessment
- Prioritized focus and investment for early and high impact
- Event monitoring and investigation

Accountability

- Enterprise-wide ownership, responsibility, and participation
- Distributed responsibility for funding and executing IRM/InfoSec solutions and processes

Sustainability

- Defined, continuous operational solutions and processes
- Automated balanced, coordinated, and cost-effective solutions to protect and enable the enterprise
- Preservation: Maintain to current levels and for enterprise changes (organizational and technological)

Advice of a Career Consultant

**"If nobody is minding the store,
someone will surely steal the goods"**

Me!

The one thing you can do to immediately strengthen security without risking unintended denials of access is to initiate aggressive monitoring and investigation.

What you see will surprise you! The visibility will convince you! The implications will motivate you.

You need to determine what you don't know before you can do anything meaningful!

A Final Keystone Issue

A Final Keystone Issue: Balance Required

C I A

Two-Part Presentation

Concerns

Actions

Take Charge

- As you move into the action phase
  - You need to take the lead to set the foundations
  - Prepare and obtain top level management support for a foundational Security Implementation & Administration Policies document
  - Actions must be based upon what you see and what needs to be controlled as defined by your document
  - What do you look for and how do you move towards the target state of control and compliance?
  - Automate the review and enforcement of controls both existing and those established during this ongoing process

Common IT General Control Deficiencies

Excessive Access to Systems / Databases

- Developer / programmer access to production environment
- Developer / programmer access to production data
- DBA access
- System Administrator access

Lack of Access Controls

- User provisioning and administration
  - Changes in responsibilities
  - Changes in organization
  - Terminations
- No documented access policies and standards
- General monitoring of the security infrastructure

Technology can help

- Define the security policy in monitoring tools
  - Operating system and security settings against baselines
  - Operating system and security changes against baselines
  - Data access against standards
  - Access by technicians should fit production profile
  - etc.
- In case of conflict
  - Deny the action, prevent the change from taking place, or
  - Issue a real-time message to data security officer, or
  - Generate an exception report for review by management
- Document
  - Baseline or security standard
  - Exceptions and transgressions

Baseline

- Why establish a baseline
  - Each system will have specific and different characteristics
  - Know where you started
  - Know where you are headed
  - Know where you have gotten
- Examples
  - Freeze an image of your operating system
  - Unload a copy of your security definitions

Baselines

- Use the baselines to create “Where we are”
- **Examples to consider**
  - **z/OS Integrity**
    - **z/OS itself**
    - **System Critical Datasets**
    - **Authorized Libraries**
    - **Program Properties Table (PPT)**
    - **Command Authority (System, Operator)**
    - **User Supervisor Calls (SVCs)**
  - ESM
    - ESM System Options
    - Critical User Attribute (CUA)
    - Public Data Sets and Resources
    - Password (Default and Trivial)
    - ESM Common Problems
- What do these look like?

System Information

```
System settings and software levels                                  Line 2 of 63
Command ===> _____________________________________________ Scroll===> CSR

   Complex  System   Collect timestamp
   S0W1     S0W1     10 Feb 2008 10:24

System identification                    Configuration parameters
Sysplex name                  SVSCPLEX MVS load parameter            0CE3W1M
Hardware name                 VM-TOKEN Initial Program Load device   1000
Logical Partition name                 Initial Program Load volume   VIMVSB
Virtual machine userid        ETPRP8I  MVS I/O configuration id      00
VM system name                SVSCVM1  Initial Program Load date     Saturday
JES node name                 SMPOMVB  Initial Program Load date     26Jan2008
VTAM net identifier           USIBMUZ  Initial Program Load time     18:18
Time zone relative to GMT     -06:00   IODF configuration id         MVS
CPU processor type            2094     IODF configuration date       20Jun2007
CPU processor model byte      D8       IODF configuration time       19:14
CPU serial (starts with LPAR) 14655    &SYSCLONE, short for SYSNAME  W1
CPU model name                IBM 2094 model S28-720

Software levels
Operating system vendor       IBM CORP
Operating system              z/OS
OS   Operating system version 1.8.0
```

System SMF Information

```
SMF parameters                                MVS and DFP options
Current SMFPRM suffix                         Multi Level Alias qualifiers    1
SMF recording active              Yes         All linklist authorized       Yes
Max Job Wait Time     HH:MM       24:00       Jobcat / stepcat enabled      No
Max SMF not yet on disk MM:SS        30:00
SMF 23/status each    HH:MM:SS    00:30:00    TSO parameters
SMF 17/scratch also temp dsn      No          Current TSO parameter source  IKJTSO00
Halt sys if SMF buffers full      No          TSO maximum number of users      10
Halt sys if last SMF dataset      No          TSO maximum reconnect minutes     3
SMF restart after dump abend      Yes         Encrypt TSO/VTAM buffers      Yes
Dflt 64bit MEMLIMIT(MB)                   0   TSO ACB password present      No

SMF recording data set                        Volume    Size  Blocks  %U Active
SYS1.S0W1.MAN1                                VPMVSB   14400    3600   0 No
SYS1.S0W1.MAN2                                VPMVSB   14400    3600  43 Yes

HSM job  Migr pfx Bkup pfx RACFind BkupProf MulTpVol TpSelVol Erase SMF
DFHSM    DFHSM    DFHSM    No      Yes      No       No       No    240
```

System SMF Information

```
SMF subsystem-dependent settings                                  Line 17 of 421
Command ===> _____________________________________________ Scroll===> CSR

  Complex  System   SMF subsystems Audit concerns Priority
  S0W1     S0W1                  4              4        5
  Pri Subs Su# Wr# Pa# Ex# Det Interval Recording activity summary
    5 SYS   11 245   0  12 Yes 00:30:00 Write 0:15 20:61 64 70:255
 Exit     Address  Record  Act Record description
                   16      No  DFSORT Statistics
                   17      No  Scratch Data Set Status
                   18      No  Rename Data Set Status
                   19      No  Direct Access Volume
                   20      Yes Job Initiation
                   21      Yes Error Statistics by Volume
 Audit concern
 Dataset activity not recorded

 Data set activity not recorded

 One or more types of data set activity records (record types 14-15,
 17-18, 60-62, 64-67) are suppressed. the product is not able to
 analyze all data set activities.
```

System IPL Information

```
Effective LOADxx cards

IODF     00 SYS1     MVS      00 Y
SYSPARM  (00,LV,SV,VN)
SYSCAT   VPMVSB113CMASTERV.CATALOG
IEASYM   (W1,SV,VN)
SYSPLEX  SVSCPLEX
PARMLIB  VENDOR.PARMLIB
PARMLIB  SVTSC.PARMLIB
PARMLIB  LVL0.PARMLIB
PARMLIB  SYS1.PARMLIB
NUCLSTB  SVN
```

```
Effective system IPL parameters
Command ===> ____________________________________________
                                                      10

   Complex  System   Collect timestamp
   S0W1     S0W1     10 Feb 2008 10:24

Operator-specified IPL parameters
SYSP=(00,LV,SV,VN)

Security related flags
Prompt operator at IPL     OPI Yes
Linklist authorized    LNKAUTH Yes
Create Link Pack Area     CLPA Yes
Clear VIO                 CVIO
Master JCL from linklib        No
LOADxx PARMLIBs used           Yes

Suffix parameters
IEASYSxx suffixes         SYSP (00,LV,SV,VN)
ALLOCxx suffixes         ALLOC
IEAAPFxx suffix            APF
CEEPRMxx suffixes          CEE
CLOCKxx suffix           CLOCK SV
COMMNDxx suffixes          CMD (J2,00,LV,SV,VN,I8)
```

System Critical Datasets

- Many system datasets and activities are critical to overall security and effectiveness.
- **SYS1.PARMLIB**
  - The IEASYSxx member of SYS1.PARMLIB contains controlling system parameters that specify how other members are to be used by the system as well as certain operating characteristics.
- **SMF Datasets**
  - Certain system libraries are instrumental to the operation of MVS providing controlling parameters as well as history and audit trail functions. Any violation of those datasets could severely impact system reliability and personnel accountability.
- **Master Catalog**
  - The MVS Master Catalog contains indices used to reference other catalogs and data groups. Write access to the Master Catalog should be restricted. Such access could potentially damage strategic information or, perhaps, render the system unusable.

System Critical Datasets – Automatically Checked

- APF data sets
- LPA data sets
- Page data sets
- Swap data sets
- ESM data sets
- RRSF data sets
- SMF recording data sets
- System dump data set
- TSO user administration data set UADS
- SYS1.NUCLEUS and SYS1.LPALIB
- JES2 and JES3 checkpoint data sets
- JES2 and JES3 spool data sets
- JES2 and JES3 parameter data set
- JES2 and JES3 STC/TSU proclib
- MSTR proclib
- MSTR parameter library
- MSTR VIO administration
- DFHSM data set BCDS, MCDS, OCDS
- HFS data sets
- DMS database DMSFILES
- DMS authorized parameter library
- DMS default parameter library
- CA1 tape management catalog TMC
- DFSMS SCDS and ACDS (integrity)
- IODF file, if DSN could be found
- Couple data sets
- RMM control dataset
- TLMS volume master file VMF
- ABR archive control file ACF

System Sensitive Datasets

```
Profiles covering sensitive data sets                                                    Line 1 of 90
Command ===> ____________________________________________________________________ Scroll===> CSR

  Complex  Timestamp        Profiles Audit concerns Priority
  S0W1     22 Feb 2008 08:48      90            89      100
  Pri Profile key                            UACC    Era S/F Audit concern
_ 100 SYS1.*.**                              READ    NO   C  No read audit, No update audit, Read fail audit, Update fail au
_  60 ANF.*.**                               ALTER   NO      Unprotected
_  60 AOP.*.**                               ALTER   NO      Unprotected
_  60 APM110.*.**                            ALTER   NO      Unprotected
_  60 ASN710.*.**                            ALTER   NO      Unprotected
_  60 ATH220.*.**                            ALTER   NO      Unprotected
_  60 AUT230.*.**                            ALTER   NO      Unprotected
_  60 AUT310.*.**                            ALTER   NO      Unprotected
_  60 CATALOG.*.**                           ALTER   NO      Unprotected
_  60 CBC.*.**                               ALTER   NO      Unprotected
_  60 CEE.*.**                               ALTER   NO      Unprotected
_  60 CICSTS.*.**                            ALTER   NO      Unprotected
_  60 CICSTS22.*.**                          ALTER   NO      Unprotected
_  60 CICSTS23.*.**                          ALTER   NO      Unprotected
_  60 CKR.**                                 ALTER   NO   R  No update audit, UACC too high
_  60 CONSUL.**                              ALTER   NO   R  No update audit, UACC too high
```

System Sensitive Datasets – SYS1

```
Profiles covering sensitive data sets                                          Lin
Command ===> ____________________________________________________________________ Scr

 Type    Sensitivity Volume Profile key / data set name
  nvsam              VPWK07 SYS1.TRACE
  nvsam  TSO UADS    VPMVSB SYS1.UADS
  notfnd NoAPFnotMnt VTMVAB SYS1.VTAMLIB
  nvsam  APF library VTMVSH SYS1.VTAMLIB
  nvsam              VTMVSC SYS1.VTAMLST

 User/grp Access  WhenProg
_ RACFADM  OWNER
_ TEDWESL  UPDATE
_ SYS1     ALTER
_ GRPTEST  ALTER
_ GROUP1   ALTER
_ GROUPZ   ALTER

 Profile attributes
 Security complex name        S0W1
 Universal access authority   READ
 Erase-on-scratch             NO
 Audit access success/failures  C

 Audit concern
 Relative audit priority      100
 Audit concern                No read audit, No update audit, Read fail audit, Update fail audit, UACC too high
```

Authorized Libraries

- Many system functions are sensitive and access to these functions must be restricted to authorized program to avoid compromising the security and integrity of the system and these programs are contain in authorized libraries.
- LPA & LINKLIST Libraries
- APF List
- INSPECT:
  - Access higher than read as it is not needed for these libraries
  - Users with access higher that read
  - Protection of dynamic APF (SETPROG) – Review ESM definitions
    - ESM FACILTY definitions CSVAPF.**
    - ESM OPERCMDS definitions for SET or SETPROG command
  - LNKAUTH=APFTAB (more restrictive) versus LNKAUTH=LNKLST

Authorized Libraries

Complex	System	APF data sets	Audit concerns	Priority
S0W1	S0W1	192	66	5

Pri	Dataset	VolSer	Sensitivity	APF	APFlist	LPA	Lnk	Lnkauth	Audit concern
2	TCPIP.SEZALNK2	VTMVAB	NoAPFnotMnt		APFlist				In APFlist but volume not mounte
2	TCPIP.SEZALPA	VTMVAB	NoAPFnotMnt		APFlist				In APFlist but volume not mounte
2	TCPIP.SEZATCP	VTMVAB	NoAPFnotMnt		APFlist				In APFlist but volume not mounte
	APM110.SFBIAUTH	VTAPMA	APF library	APF	APFlist				
	ASN710.SASNALNK	VTD71A	APF library	APF	APFlist				
	ASN710.SASNLLNK	VTD71A	APF library	APF	APFlist				
	ATH220.SATHLOAD	VTATHC	APF library	APF	APFlist				
	AUT230.SINGMOD3	VTAUTD	LPA list	APF		17			
	BJT.V2R1M0.SBJTLOAD	VPWK03	APF library	APF	APFlist				
	CAN390.BASE.RKANMOD	VPCANA	APF library	APF	APFlist				
	CAN390.S0W1.RKANMOD	VPCANA	APF lib+Lnk	APF	APFlist		55	Lnkauth	
	CAN390.TKANMOD	VTCANA	APF lib+Lnk	APF	APFlist		54	Lnkauth	
	CAN390.TKANMODL	VTCANA	APF library	APF	APFlist				
	CBC.SCCNCMP	VTMVSE	APF Linklst	APF			31	Lnkauth	

Program Properties Table (PPT)

- Many programs, predominantly in the system software area, require specific characteristics. To facilitate this requirement, MVS contains a facility that enables certain properties to be attributed to specific programs. Such properties as non-cancelability and non-swappability are important to ensure the effectiveness of online systems. An extreme characteristic that may be permitted, is the ability to bypass password security restrictions.
- Each entry in the Program Properties Table (PPT) describes one program and assigns that program certain attributes or privileges.
- The two attributes of concern are:
  - The bypass password attribute (PASS vs. NOPASS), that indicates that the indicated program can bypass dataset security
  - Privilege Protect Key specifies a number from 0 – 15 which controls what memory the program can update.
    - Most non-privileged programs execute with protect key of 8
    - Protect key values of 0 – 7 are considered “privileged” and permit the program to obtain all the privileges of the operation system. Once a program has this privilege it can bypass security of the system.

```
Program Property Table                                          Line 1 of 13
Command ===> ____________________________________________ Scroll===> PAGE
                                                 10 Feb 2008 10:24
   Complex  System   Count Audit concerns Priority
   SOW1     SOW1        91             85        8
   Pri Program  Key Bypass NoDSI Modif NonSwap NonCan Priv Systask Audit concer
     6 CQMMAIN    7              Modif                              Executes in

Program name (must be APF)     CQMMAIN
Job step storage key             7
Bypass password / SAF          No
No data set integrity          No
Default entry IEFSDPPT         No
Non-swappable                  No
Non-cancellable                No
Privileged (no SWAP)           No
System task not timed          No

Audit concern
Executes in system key, Modified from IEFSDPPT
 Executes in system key

 The task runs in a system key. This authorizes the task to bypass
 system security.

  Modified from IEFSDPPT

  The PPT entry was modified from the system default.
```

Command Authority

- Execution of operator and/or system commands should be controlled by ESM
- INSPECT:
  - JES2 parameters for command authority on:
    - INTRDR
    - JOBCLASS
    - TSUCLASS
    - STCCLASS
  - SDSF
  - Netview
  - Check for other products bypassing ESM for operation and/or system commands, like Omegamon etc.

```
JES2 Job Class parameters (e.g. MVS command auth / BLP)          Line 1 of 19
Command ===> ____________________________________________________ Scroll===> PAGE

   Complex  System   Subsys Classes Audit concerns Priority
   S0W1     S0W1     JES2        36              36        20
   Pri C Command Auth commands    BLP HOLD ACCT Time      Regio SWA   PL UJP U
    20 A VERIFY  ALL              Yes No   No   001440,00 0001M ABOVE 00 Yes Y

Command disposition   COMMAND VERIFY
Authorized cmd groups    AUTH ALL
Bypass Label Processing   BLP Yes
Jobs held until released HOLD No
Account number required  ACCT No
Time limit               TIME 001440,00
Region size            REGION 0001M
SWA ctrl block residency  SWA ABOVE
PROCxx suffix         PROCLIB 00
Job purge exit taken   IEFUJP Yes
SYSOUT limit exit actv IEFUSO Yes
SMF Type 6 written      TYPE6 Yes
SMF Type 26 written    TYPE26 Yes

Audit concern
BLP allowed; TAPEVOL not active, will not test ICHBLP, MVS Modify commands
allowed, RACF-protected but low OPERCMDS default RC, verified by operator, No
account numbers required
 BLP allowed; TAPEVOL not active, will not test ICHBLP

 BLP is allowed for the job class, but the RACF TAPEVOL class is not
 active. BLP is not RACF-protected. Whether the FACILITY ICHBLP
 resource is protected or not is irrelevant, it will not be checked.

 MVS Modify commands allowed

 MVS console, system, or I/O commands are allowed in the job class.
 RACF-protected but low OPERCMDS default RC

 RACF is configured to protect the MVS commands by using profiles in
 the OPERCMDS class. However, no catchall profile (a profile with
 key=*.**, key=* or key=**) for this class is defined, and the default
 RC is too low, possibly allowing access.
```

JES2 / Opercmds / SDSF

Name	Summary	Records	Title
GLOBAL	0	0	zSecure Admin+Audit for RACF JES control profiles
JESINPUT	0	0	zSecure Admin+Audit for RACF JES input sources for j
FACILITY	0	0	zSecure Admin+Audit for RACF JES RACF validation of
JESJOBS	0	0	zSecure Admin+Audit for RACF JES submit and cancel c
JESSPOOL	9	9	zSecure Admin+Audit for RACF JES sysin/sysout datase
NODES	0	0	zSecure Admin+Audit for RACF JES validation of inbou
WRITER	0	0	zSecure Admin+Audit for RACF JES outbound data contr
PROPCNTL	1	1	zSecure Admin+Audit for RACF JES userid propagation
SURROGAT	45	45	zSecure Admin+Audit for RACF JES surrogate submit co

Complex	Class	Profile key
SOW1	OPERCMDS	JES2.**
SOW1	OPERCMDS	JES2.START.DEV
SOW1	OPERCMDS	JUNK.START
SOW1	OPERCMDS	MVS.**
SOW1	OPERCMDS	MVS.ACTIVATE
SOW1	OPERCMDS	RACF.**
SOW1	OPERCMDS	RACF.RESTART.**
SOW1	OPERCMDS	RACF.SET.**
SOW1	OPERCMDS	RACF.STOP.**
SOW1	OPERCMDS	RACF.TARGET.**

Complex	Class	Profile key
SOW1	SDSF	ISFATTR.**
SOW1	SDSF	ISFAUTH.**
SOW1	SDSF	ISFAUTH.%*.DATA
SOW1	SDSF	ISFAUTH.%*.TEDS.*
SOW1	SDSF	ISFCMD.**
SOW1	SDSF	ISFCMD.DSP.**
SOW1	SDSF	ISFCMD.ODSP.**
SOW1	SDSF	ISFCMD.ODSP.HCHECKER.SOW1
SOW1	SDSF	ISFINIT.**
SOW1	SDSF	ISFOPER.**

SuperVisor Calls (SVCs)

- Supervisor call (SVC) is a processor instruction that directs the processor to pass control of the computer to the operating system's supervisor program. System vs user-written.
- The coding of SVCs require exceptional assembler skills and usually lead to compromising z/OS integrity. Many vendors and customer have problems with their SVCs.
  - Most of them are defined statically in SYS1.PARMLIB (IEASVCxx)
  - Sometimes dynamically defined / hooked in
- INSPECT:
  - Software products use of SVC and request a "statement of integrity" – especially if vendor written (user SVC)
  - Use of assembler compilers on production system. Monitor use
  - Review IPL messages for IEASVC00 messages indicating SVCs that are not found

```
Supervisor Call Audit Display                                        Line 1 of 33
Command ===> ____________________________________________ Scroll===> PAGE
scroll right for more info
   Complex  System   Routines SVCs ESRs Audit concerns Priority
   SOW1     SOW1          143  109   34            136       25
   Pri SVC ES# APF Where    K SP  Program  U Sf InstrSc Function
    25  51     No  EPLPA          IGC0005A 1      M     SNAP/SDUMP
Idx  Where   Key SP  Program  InstrSc Eye catchers
CN I EPLPA           IGC0005A   M     ..IEAVAD00 06180UA27431..-{Q..0xM..
  O  PVT                               ..
Appl     Result
MVS
SVCUPDTE Sf Last update Caller   Where   Module
       1                0009CEDA PVT
Index    Typ APF ESR Att Locks
Current: 3/4 No  No    A   L
Old:     3/4 No  No    A   L
Expect:  3/4 No  No  ??? ???
Instruction/Str/SVC scan results
ModeSupRB   No  131: RACINIT
                132: RACLIST/ICHEINTY
Audit concern
Instruction scan hit, SVC scan hit, Caller may be unauthorized, Updated during
NIP
First 256 bytes of SVC
0000. A7F4000D 15C9C5C1 E5C1C4F0 F040F0F6 *x4...IEAVAD00 06*
0010. F1F8F0E4 C1F2F7F4 F3F10700 A7C50004 *180UA27431..xE..*
0020. 033D3C7C 58CC0000 58600380 90E36010 *...@.....-...T-.*
```

Caller may be unauthorized

Any program may call the SVC. This is true for most SVCs. By itself, it is not a cause for concern, unless the SVC performs sensitive actions, in which case it should check the authorization of the caller itself. If an installation-defined SVC should only be used by authorized programs, it should not be callable by

Baselines

- Use the baselines to create “Where we are”
- Examples to consider
  - z/OS Integrity
    - z/OS itself
    - System Critical Datasets
    - Authorized Libraries
    - Program Properties Table (PPT)
    - Command Authority (System, Operator)
    - User Supervisor Calls (SVCs)
  - **ESM**
    - **ESM System Options**
    - **Critical User Attribute (CUA)**
    - **Public Data Sets and Resources**
    - **Password (Default and Trivial)**
    - **Common ESM Problems**
- What do these look like?

ESM Systems Options (SETROPTS)

- The SETROPTS list contains installation options that impact the manner in which security is installed in your environment.

Pri	Complex	System	Count
35	S0W1	S0W1	12

Pri	Parameter	Value	Audit concern
35	PROTECTALL	No	The security system is not even invoked for each dataset / not C2 compliant
30	BATCHALLRACF	No	Allowing unidentified batch work makes hacking easy / not C1 compliant
25	TAPEVOL	No	Tape volumes are unprotected / not C1 compliant
21	SAUDIT	No	Administrator activity undetectable
20	OPERAUDIT	No	OPERATIONS activity undetectable
15	CMDVIOL	No	Attempts to change protection not audited
15	ERASEONSCRATCH	None	Disk scavenging threat not countered / not C2 compliant
15	HISTORY	No	Users can use same passwords over and over
11	MINCHANGE	No	Without MINCHANGE users can thwart the PWDHISTORY more easily
11	RVARYSTATUSPWSET	No	Password to deactivate RACF still at IBM default
10	GENERICOWNER	No	User with CLAUTH can bypass generic profiles / not B1 compliant
10	RVARYSWITCHPWSET	No	Password to switch RACF database still at IBM default

Critical User Attributes (CUA)

- Critical User Attributes are these attributes that provide a user with extended capabilities such as:
  - Security administration functions
  - Unix System Services (e.g., UID(0)

```
Users with uid 0                                                    Line 1 of 56
Command ===> ____________________________________________________ Scroll===> CSR

   Complex  Timestamp       Users with uid 0
   SOW1     23Feb2008 08:48                56
   Userid   OMVS uid   Name                 Owner    RIRP SOA LastConDa LastPwd
__ ANDREWM  _________0 ANDREW MCINTYRE      GROUP1        Y Y 05Feb2008 13Apr20
__ ARSSERVR _________0 ARS SERVER ID        ARS       Y       19Nov2001
__ BERGHA   _________0 JULIE BERGH          $RACFGRP      YYY 23Feb2008 22May20
__ BERGHD   _________0 JULIE                $RACFGRP YY   YYY
__ BERGHJ   _________0 JULIE                $RACFGRP      YYY 23Feb2008 18Jun20
   BOILES1          0 CARLOS BOILES        GROUP1          Y
```

Public Access to Data Sets and Resources

- Evaluate the need for a data set or general resources with a UACC value higher than NONE
  - It may have been acceptable before, but remember the HTTP server on z/OS can read data sets as well.
- INSPECT
  - The need for Universal Access definition
  - Use of ESM global access control for data sets and resources
  - Data sets that have UACC higher than NONE
    - SYS1.PARMLIB
    - SYS1.PROCLIB

RACF profile audit concerns

Command ===> _____

Complex	Timestamp	Audit concerns	Priority
S0W1	22Feb2008 05:36	226	10

	Pri	Class	Profile key	Audit concern
__	10	FACILITY	STGADMIN.**	Verify why UACC>=UPDATE
__	10	FACILITY	WHATS.IT	Verify why UACC>=UPDATE
__	10	FACILITY	WYUWUI.*	Verify why UACC>=UPDATE
__	10	IBMOPC	**	Verify why UACC>=UPDATE
__	10	OPERCMDS	JES2.**	Verify why UACC>=UPDATE
__	10	OPERCMDS	JES2.START.DEV	Verify why UACC>=UPDATE
__	10	OPERCMDS	JUNK.START	Verify why UACC>=UPDATE
__	10	OPERCMDS	MVS.**	Verify why UACC>=UPDATE
__	10	OPERCMDS	MVS.ACTIVATE	Verify why UACC>=UPDATE
__	10	PROGRAM	*	Verify why UACC>=UPDATE
__	10	SDSF	ISFATTR.**	Verify why UACC>=UPDATE
__	10	SDSF	ISFAUTH.**	Verify why UACC>=UPDATE
__	10	SDSF	ISFAUTH.%*.TEDS.*	Verify why UACC>=UPDATE
__	10	SDSF	ISFCMD.**	Verify why UACC>=UPDATE
__	10	SDSF	ISFCMD.DSP.**	Verify why UACC>=UPDATE
__	10	SDSF	ISFCMD.ODSP.**	Verify why UACC>=UPDATE
__	10	SDSF	ISFINIT.**	Verify why UACC>=UPDATE
__	10	SDSF	ISFOPER.**	Verify why UACC>=UPDATE
__	10	TSOAUTH	MOUNT	Verify why UACC>=UPDATE

Passwords

- Password quality is still a major concern
  - ESM options for length and contents
  - ESM exits can augment; content filtering for trivial passwords
- INSPECT:
  - ESM PASSWORD options
  - ESM exits implemented to augment password control (dictionary attack)
  - Procedure for ESM user definitions
  - What is a the default/initial password

Passwords

```
Enter "/" to select report(s)
_  TRUSTED          - Users who can bypass normal system security
_  SYSTEM AUTH      - Users with special authority system-wide
_  GROUP AUTHORITY- Users with special authority to groups
_  SHARED UNIX IDS- Users that share a uid, groups that share a gid
_  PASSWD INTERVAL- Users with long password interval or nointerval
_  PASSWD EXPIRED - Users with expired password
_  INITIAL PASSWD - Users with an initial password
_  PWAGE SUMMARY  - Password age overview
_  PWAGE DETAILS  - Password age details (detailed report only)
_  LOGON FAILURES - Users with password failures
_  NEVER LOGGED ON- Users that never logged on
_  PENDING REVOKE - Users with pending revoke
_  LAST LOGON SUM - Last logon overview
_  LAST LOGON DET - Last logon details (detailed report only)

/  Password          Userids with trivial passwords (not from an unl

  /* select non-revoked users with weak DES password */
  select class=user segment=base key=(AOLSSON,
     ARG003,ARSSERVR,ASAMMAR,ASCR1,ATORTOR,AUTOID,BETHM,
     BOILES1,CGARNER,CICSDB2,CICSTS12,CICSTS22,CLARK,DAFFRON,
     DAJJ,DB2PM,DCEKERN,DDDD,DFHSM,DFS,DOMEA,
     DPLEMON,DSSISTC,GARNERC,GDAFFRN,GHARDY,IBMAPL,IBMAPL3,
```

Common ESM Problems

- **USER/GROUP Maintenance**
  - Finding user and grouping inconsistencies
- **PROGRAM Class Maintenance**
  - Check for obsolete conditional permission lists when program definitions have been removed
  - Check for non-existent data set/volume program combinations
  - Checking for program definitions not describing any physical module
- **DATASET Maintenance**
  - Finding and protecting unprotected data sets checks depending on the current protection setting
  - Removing unused discrete definitions - resulting from volume-level operations
  - Finding and removing redundant discrete definitions
  - Removing unused generic definitions (after deletion of 'subject' data sets)
  - Finding and resetting unnecessary ESM-indicated bits (where no discrete definition exists)
- **STARTED Class Maintenance**
  - Finding inconsistencies in started task definitions

Examples of ESM Clean-Up

```
BERGHA.C2R195D.CKRCMD                                    Columr
=> ____________________________________________________ Scr
********************************* Top of Data ****************
     /* CKRCMD file CKR1CMD complex S0W1 NJE SMPOMVB g
     /* Commands generated by VERIFY ONVOLUME    */
    deldsd 'SVTSCU.TEST' vol(VPWRKB) noset
```

Example of discrete profile defined in RACF and dataset does not exist

```
BERGHA.C2R195D.CKRCMD                                    Columns 0
=> ____________________________________________________ Scroll
     ralter program JUNK     delmem('BERGHJ.JUNK1')
     ralter program JUNK     delmem('BERGHJ.JUNK2')
```

Example of programs defined in the PROGRAM class and they do not exist

```
BERGHA.C2R195D.CKRCMD
=> ____________________________________________________
     rdelete started IBMSTC.*
     rdelete started IBMSTC1.*
```

Example of obsolete started task definition

Beyond Baseline: Clean up and Control

- Now you have use the baselines – you can clean up
- BUT
  - How do you maintain and prevent re-contamination?
  - After the fact – clean up
    - using SMF event reporting
    - Utilizing your baseline comparison reports
  - Before the fact – prevent the problem
    - Once your policies are defined and codified
    - Establish a means to prevent conditions outside the policies from taking place – control and verify commands, before their execution can undo

Beyond Baseline - Control

- ESM enforces controls consistent with its architecture
- ESM allows events contrary to your policy
  - Control the commands BEFORE they cause problems
    - Prevent
    - Modify
    - Additional pre/post commands

    - Extend or reduce the security level of the issuer (sub-delegate ESM authorities

Beyond Baselines – Maintenance

- z/OS is an evolving platform
- Technical expertise and awareness is paramount
- Honing skills must be ongoing
- Products employed to evaluate and control must grow
- Automate processes where possible –
  - Machine speed / reaction time
  - Repetitive tasks
  - Consistent and continuous monitoring to enable timely detection and enforcement

Beyond Baselines – Moving Forward

- Now
  - Baselines to measure progress
  - Baselines to compare changes
  - Clean up the environment
  - Prevent subsequent contamination

- You can answer the question:

How Secure is My Mainframe?

QUESTIONS

?