Agenda

- Introduction
- Objectives
- What's Hardware?
- IOCDS and IODF
- Common Hardware Configurations
- Security Controls
- What do we need to do?
- Summary
- Questions

IBM Mainframe
Are they really secure?

Introduction

Introduction

- Mark Wilson
  - Technical Director at RSM Partners
  - I am a mainframe technician who's specialist subject is Mainframe Security
  - I have been doing this for over 30 years (35 to be precise ☺)
  - This is part six of seven one hour long sessions on mainframe security
  - Full details can be seen on the New Era Website:
    - http://www.newera-info.com/MF-SEC.html

My passions outside of work?

- One wife and three daughters…..enough said…..don't have anytime or money for anything else….or so they tell me ☺
- Motorbikes
  - www.wilson-mark.co.uk
- Football
  - www.wba.co.uk
- Scuba Diving
  - Way too many links to list here…..But I have been and dived here
  - http://en.wikipedia.org/wiki/Chuuk_Lagoon

OBJECTIVES

Objectives

- High level look at some potential hardware related risks that could be exploited if we don't build our infrastructure correctly
- Discuss the risks/issues that we have encountered within some of our clients over the years
- Give you plenty of information that you can go and research…..

What's Hardware?

What's Hardware?

- Anything that we can touch, that plugs into our mainframe
  - Processor(s)
  - Disk aka DASD
  - Cart/Tape (Real or Virtual)
  - Printers (really!!)
  - OSA's
  - FICON/ESCON
  - Switches
  - Anything else that I may have forgotten ☺

SPECIALISTS RSM

EAL

- Evaluation Assurance Level
  - IBM spend a lot of money getting z hardware tested and certified, certain configurations
  - Currently at EAL 5+
- How many of you know what this is?
  - You need to know what this is if you are designing hardware solutions
- How many have looked at it?
  - You need to
- Simple GOOGLE search shows plenty of reading

SPECIALISTS RSM

IOCDS and IODF

SPECIALISTS RSM

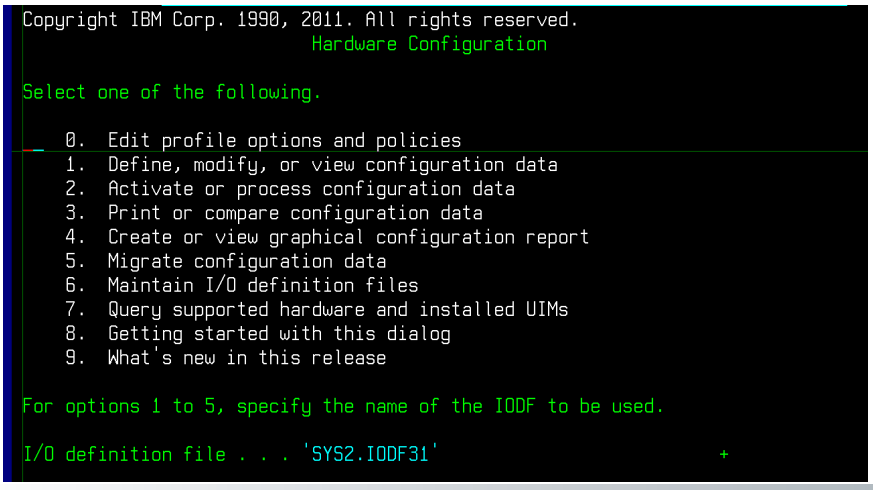
IOCDS and IODF in Simple Terms

- The IOCDS describes your hardware configuration to the physical CPC hardware
  - It contains definitions of your LPARs, channels, peripherals, etc. so the hardware knows how it is configured and what devices are attached to it
- The IODF describes your hardware configuration to the operating system (z/OS)
  - It contains definitions of your LPARs, channels, peripherals, etc. so the operating system knows how the hardware is configured and what is attached to it
  - The IODF also contains information only the OS needs to be concerned with such as EDTs, whether a UCB should be online at IPL, etc.

IODF

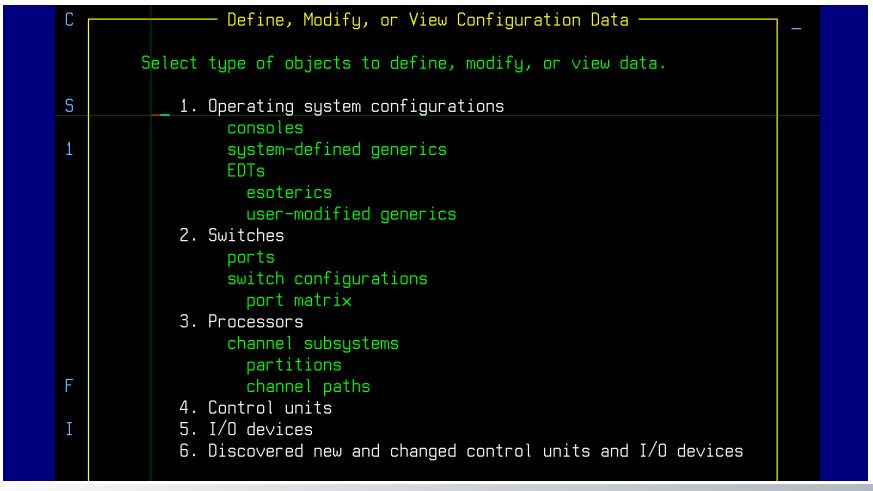
- Typically built using the HCD ISPF dialogs, but can be built from source control datasets
- This is how we did it in the old days as mentioned it describes the h/w configuration for the operating system
- Contains the relationships between LPAR, PCHIDs, CHIPIDs, Controllers and Devices (Disk, Tape, Switches, Printers, etc)
- Very common to have several IODFs sometimes shared between multiple LPARs or SYSPLEXs
- Usually managed and maintained by the system programmers, but in large organisations there can be a dedicated hardware team

IODF Screenshot from HCD



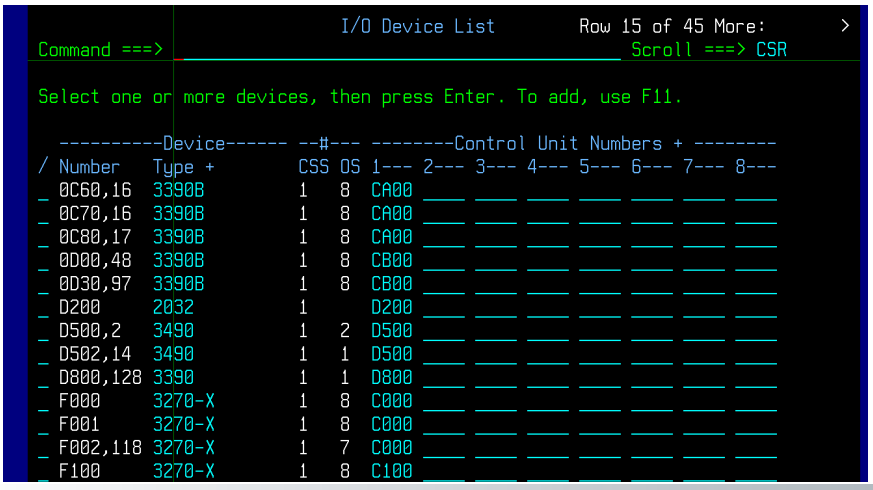
SPECIALISTS RSM

IODF Screenshot from HCD



SPECIALISTS RSM

IODF Screenshot from HCD

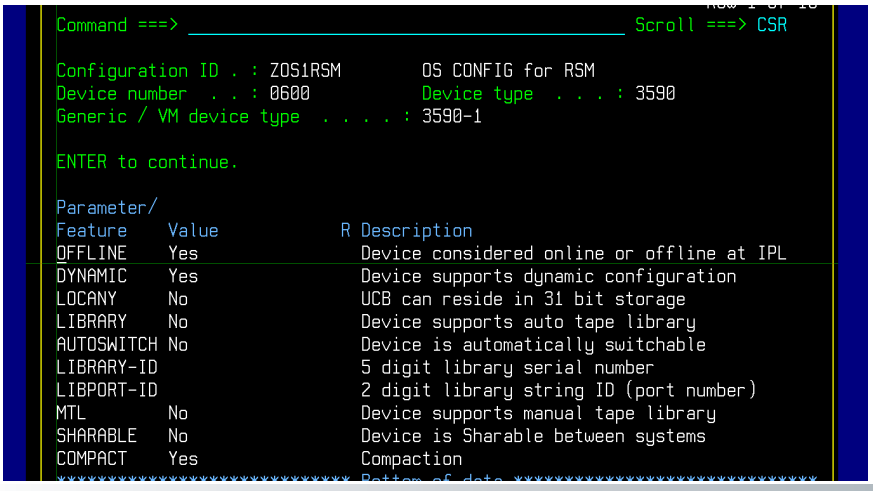


```
                          I/O Device List        Row 15 of 45 More:      >
Command ===> _____________________________________ Scroll ===> CSR

Select one or more devices, then press Enter. To add, use F11.

  ----------Device------ --#--- --------Control Unit Numbers + --------
/ Number    Type +        CSS OS 1--- 2--- 3--- 4--- 5--- 6--- 7--- 8---
_ 0C60,16   3390B         1   8  CA00 ____ ____ ____ ____ ____ ____ ____
_ 0C70,16   3390B         1   8  CA00 ____ ____ ____ ____ ____ ____ ____
_ 0C80,17   3390B         1   8  CA00 ____ ____ ____ ____ ____ ____ ____
_ 0D00,48   3390B         1   8  CB00 ____ ____ ____ ____ ____ ____ ____
_ 0D30,97   3390B         1   8  CB00 ____ ____ ____ ____ ____ ____ ____
_ D200      2032          1      D200 ____ ____ ____ ____ ____ ____ ____
_ D500,2    3490          1   2  D500 ____ ____ ____ ____ ____ ____ ____
_ D502,14   3490          1   1  D500 ____ ____ ____ ____ ____ ____ ____
_ D800,128  3390          1   1  D800 ____ ____ ____ ____ ____ ____ ____
_ F000      3270-X        1   8  C000 ____ ____ ____ ____ ____ ____ ____
_ F001      3270-X        1   8  C000 ____ ____ ____ ____ ____ ____ ____
_ F002,118  3270-X        1   7  C000 ____ ____ ____ ____ ____ ____ ____
_ F100      3270-X        1   8  C100 ____ ____ ____ ____ ____ ____ ____
```


IODF Screenshot from HCD



```
Command ===> _____________________________________ Scroll ===> CSR

Configuration ID . : ZOS1RSM        OS CONFIG for RSM
Device number  . . : 0600           Device type  . . . : 3590
Generic / VM device type  . . . . : 3590-1

ENTER to continue.

Parameter/
Feature     Value           R Description
OFFLINE     Yes               Device considered online or offline at IPL
DYNAMIC     Yes               Device supports dynamic configuration
LOCANY      No                UCB can reside in 31 bit storage
LIBRARY     No                Device supports auto tape library
AUTOSWITCH  No                Device is automatically switchable
LIBRARY-ID                    5 digit library serial number
LIBPORT-ID                    2 digit library string ID (port number)
MTL         No                Device supports manual tape library
SHARABLE    No                Device is Sharable between systems
COMPACT     Yes               Compaction
******************************* Bottom of data ********************************
```

IOCDS

- Built from a Production IODF using the HCD ISPF panels
- But you can create using a simple txt file
- IOCDS written to the processor into:
  - A0, A1, A2 or A3
- You must have a well documented process for using and swapping your IOCDs

Sample Text IOCDS

```
ID    MSG1='TEST CTC CONFIG',                                  *
            MSG2='TSGIM.IODFAA - 2010-03-22 17:19',SYSTEM=(2066,1), *
            TOK=('IWMTEST',00800003722D20861719478801l0081F00000000,*
            00000000,'10-03-22','17:19:47','TSGIM','IODFAA')
      RESOURCE PARTITION=((SOE1,1),(SOE2,2),(SOE3,3),(SOE5,4))
      CHPID PATH=(8A),SHARED,PARTITION=((SOE1,SOE2,SOE3,SOE5),(=)), *
            TYPE=CTC
      CHPID PATH=(8B),SHARED,PARTITION=((SOE1,SOE2,SOE3,SOE5),(=)), *
            TYPE=CNC
      CNTLUNIT CUNUMBR=B011,PATH=(8B),UNITADD=((00,002)),CUADD=1,   *
            UNIT=SCTC
      CNTLUNIT CUNUMBR=B019,PATH=(8D),UNITADD=((00,002)),CUADD=1,   *
            UNIT=SCTC
      IODEVICE ADDRESS=B018,UNITADD=01,CUNUMBR=(B019),STADET=Y,     *
            PARTITION=(SOE2,SOE3,SOE5),UNIT=BCTC
      IODEVICE ADDRESS=B020,UNITADD=01,CUNUMBR=(B021),STADET=Y,     *
            PARTITION=(SOE3,SOE5),UNIT=BCTC
      IODEVICE ADDRESS=B020,UNITADD=00,CUNUMBR=(B020),STADET=Y,     *
            PARTITION=(SOE1),UNIT=BCTC
```

And don't forget.....

- With careful planning and management both the IOCDS and IODF can be dynamically updated!
- Who has access to be able to do that??
- When was the last time you reviewed the controls for this?

Common Hardware Configurations – With Security Implications

To Share or Not to Share……

- That is the question….But who decides?
- How many of us get involved in the hardware design process?
- System z does it well, but you do need to consider what, how and when you share stuff…..Not only what your are sharing, but with what
- Do you have the same security controls for the two or more LPARs that may be sharing a resource
- Simple rule….. **DON'T SHARE**, unless you have to…. it **reduces** risk!

Shared DASD

- This is where we share one or more volumes across one or more LPARs, say Production and Development
- But, we don't share the same security database
- So we have a set of security controls on Production that are different to those on Development
- What we have seen is…….

Shared DASD

- Production volumes, both System and application data ones, being put online to a Development system
- A Developer or Systems Programmer then updates Production datasets on the volumes under the control of the Development RACF database
- The user in question does not have access to the required RACF dataset profiles on the Production database….
- However, they have the RACF Operations attribute on the Development RACF Database!

Shared Tape/Cart

- This is where a Tape Library is shared between two LPARS Production and QA, again it's a separate RACF database for each system
- A developer READS a Production application backup and restores the data to their teams group HLQ
- The data in question was of a sensitive nature as it contained credit card and account information
- The RACF dataset profile that protected the data allowed over 50 developers to read the sensitive data

Security Controls

SPECIALISTS RSM

Security Controls

- There are many controls available, but the first thing we need to do is understand the hardware configuration
- You need to understand it, before you can design and build the require security controls
- Some of the controls are:
  - OPERCMDS
    - VARY
    - ACTIVATE
    - There are others…you need to review…..
  - SDSF
  - APF & SVC34
  - Dataset Access to xxxx.IODFx datasets

SPECIALISTS RSM

OPERCMDS

- VARY
  - Make sure that the MVS.VARY profile/rule is defined explicitly
  - We recommend
    - Default Access of NONE (UACC in RACF Terms)
    - Enable successful Auditing, so that we get an audit trail of all MVS Vary commands issued
    - Strictly controlled ACL with only automated operations and console operators with access
    - System Programmers only get access via “Break Glass” process

OPERCMDS

- ACTIVATE
  - Make sure that the MVS.ACTIVATE profile/rule is defined explicitly
  - We recommend
    - Default Access of NONE (UACC in RACF Terms)
    - Enable successful Auditing, so that we get an audit trail of all MVS ACTIVATE commands issued
    - Strictly controlled ACL with System Operators and System Programmers having access

SDSF

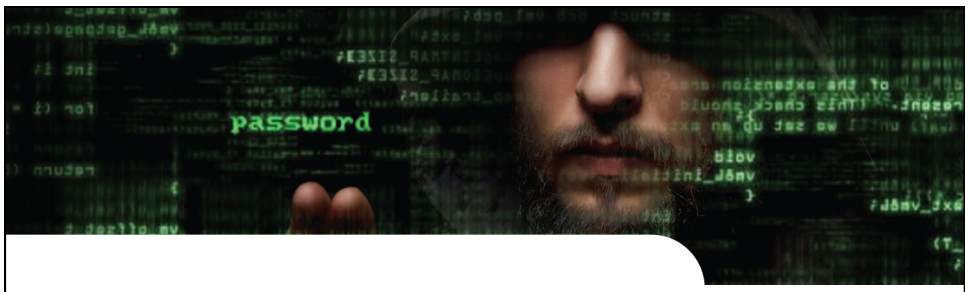
- The most effective control here is protecting access to the "/" that allows commands to be entered
- The profile/rule is ISFOPER.SYSTEM
- Ensure this is protected with you ESM
  - We recommend
    - Default Access of NONE (UACC in RACF Terms)
    - Strictly controlled ACL with only the following teams having access:
      - System Programmers
      - Console Operators
      - Hardware team

APF & SVC34

- APF
  - Same old story with APF
  - If we an update an APF authorised library we can do what we want
  - Even invoke SVC34 to issue operator commands
  - We can even make the command look like it was issued by a different user!
  - Make sure your APF libraries are tightly controlled and you have a regular review process….We have covered this before….

Dataset Access to xxxx.IODFx datasets

- You will have a naming standard
- The most common is SYS1.IODFxx
- Where xx is 00 – 99
- You need to know who has access and at what level
- Ensure this is protected with you ESM
  - We recommend
    - Default Access of NONE (UACC in RACF Terms)
    - Strictly controlled ACL with only the following teams having access:
      - System Programmers
      - Hardware team



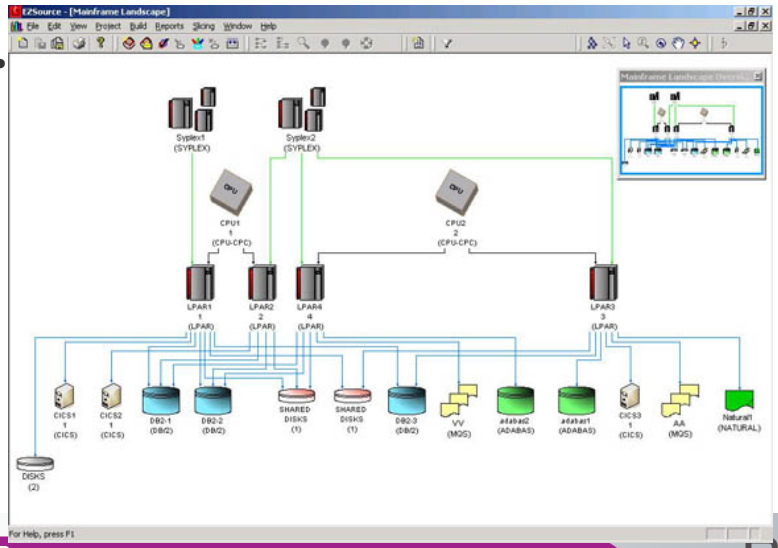
What do we need to do…….

What do we need to do….

- To stop the bad guys and Girls?
  - We need to get on the front foot..
  - You need to really understand you hardware configuration
  - Footprint the system yourself
  - Get your findings verified with the system programmers or hardware team
  - You need to know what is shared and with what…..
  - You need to fully understand the security controls that have been deployed
  - More importantly which ones HAVE NOT been deployed!

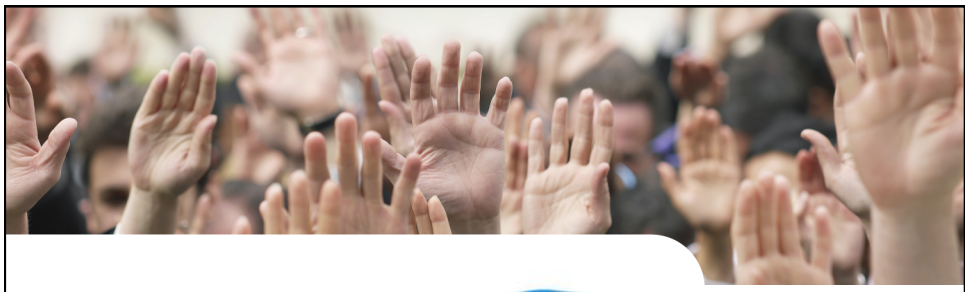
Summary

High Level View



Summary

- You need to be well informed about the end to end security configuration of your hardware
- Especially any of those “things” that may be internet facing
- If you don’t understand it how can you be certain its secure!
- You need the knowledge and then YOU must test them or get them tested
- Because today its not a case of if the bad people are in your network and looking at your applications!!!
- They are here …. we need to understand what can we do to stop them hurting us



Questions

SPECIALISTS RSM

Contact

Mark Wilson
RSM Partners
eMail: markw@rsmpartners.com

Mobile: +44 (0) 7768 617006

www.rsmpartners.com

SPECIALISTS RSM