zAuditing Essentials
Volume 1
Has The Horse Already Bolted?

Agenda

- Why should you care?
- Front Doors vs Back Doors
- What Auditors Want
- System z Foundation
- System Integrity
- Processors and Partitions
- IPLing a z/OS Logical Partition
- And Finally...

Why should you care?

- Rumours of the death of the mainframe have been greatly exaggerated leading to...
  - Serious lack of investment in new personnel
  - Skilled personnel retiring
- Consequently…
  - No new Risk Analysis on System z in recent times
  - Security policies out of step with technology use
- New focus on audit means...
  - In depth analysis skills required
  - No centralised repository of knowledge

Front Doors vs Back Doors

There are 2 entrances to most homes and businesses - the Front Door & the Back Door
What we have all been auditing and securing up until now is the Back Doors
You can have a flawless security system on your Back Door but if you don't at least close the Front Door you'll still lose your belongings to an opportunist thief
The same is true of any computer system

What is a Front Door?

- Not BAU for Auditing System z!
- One can have flawless security systems on the Back Door but, if the Front Door is not at least closed, an opportunist thief can still take your belongings
- Partly physical & logical access to devices
- Partly securing APIs
- Partly managing configuration changes
- Front Door issues can lead to non compliance with SoX!

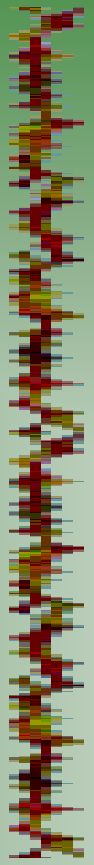
What Auditors Want

- Speaking the same language
  - Risk, Mitigation & Control
  - Confidentiality, Integrity & Availability
  - Identity Management, Access Control, Detective Control & Preventative Control
- Scope
- IODF
- Front Door issues can lead to non- compliance with Sarbanes Oxley!
- Help!

What Auditors Want

Required Skills

Audit awareness
Risk awareness
z/OS Analysis
IODF Analysis
RACF Analysis
Local data expertise
etc



Available Skills

Audit averse
Risk tolerance
Audit Analysis

Compliancy Specialism
Departmental expertise
etc

Do you know who else can get to your Production Data?

System z Foundation

- Operating System Integrity
- Operating System Choice
  - zBX, z/Linux, z/OS, z/VM, z/VSE, z/TPF
  - z/Windows soon?
  - Dynamic Configuration Changes
- External Security Manager
- 50 years and no change – really?
- IODF
  - Increasingly concern with shared CHIPIDs
- Compliance vs Security

System Integrity

- SHARE Security Project formed in 1972
- Mission:
  - Develop security requirements for future IBM Operating Systems
- Problem:
  - Any security could be bypassed if the defined Operating System Interfaces could be circumvented
- SHARE Security Project conclusion:
  - **There can be no System Security without Operating System Integrity**

System Integrity

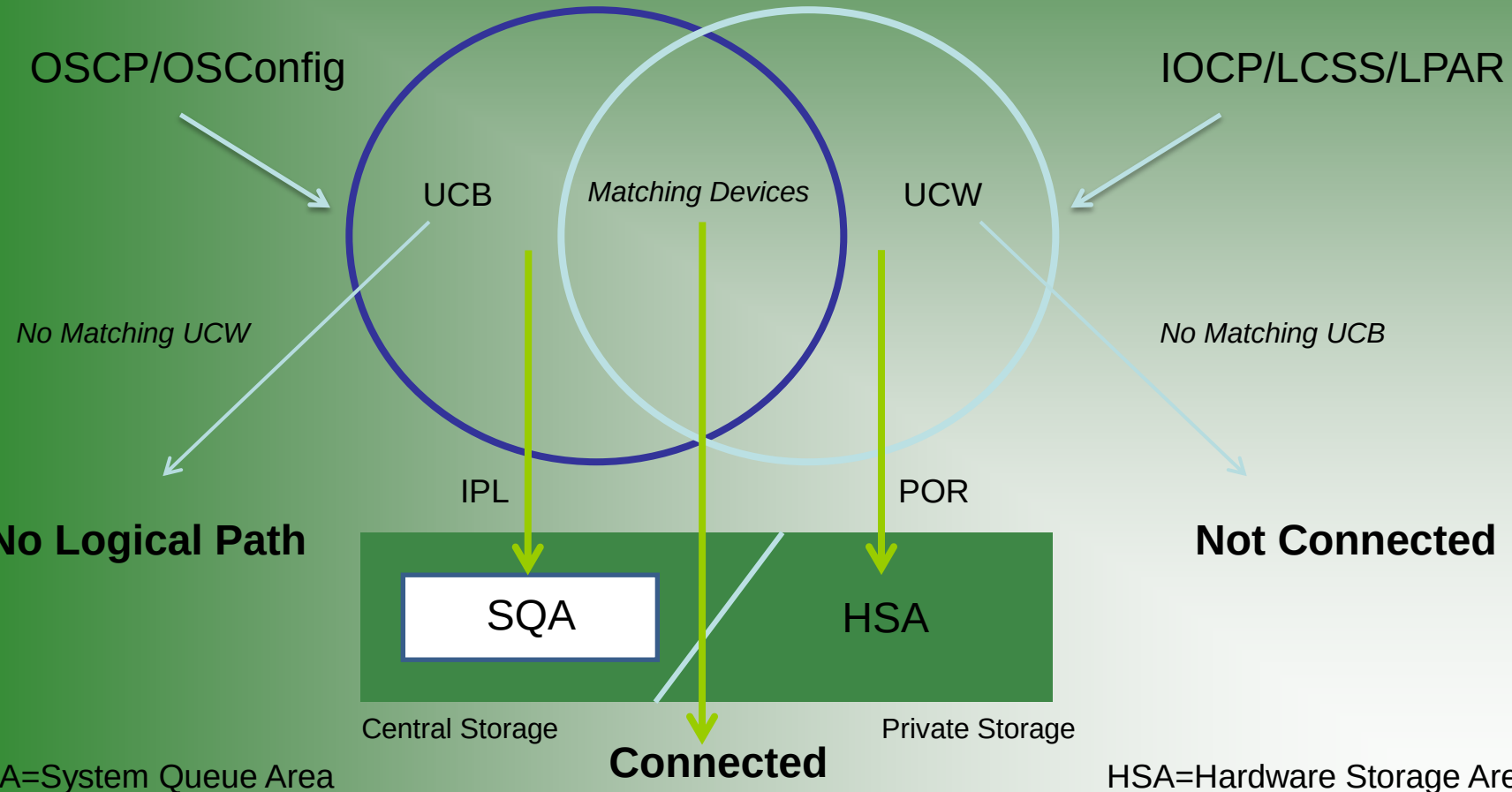
- Problem not as prevalent as in the PC world
- 75+ Vulnerabilities on most z/OS systems!
- Can’t be addressed with system settings or config
- Fixes available for most vulnerabilities
  - Security flagged APARs
  - Won’t even know about the fix if you don’t ask about the problem
- Vulnerability scans should be run on z/OS
  - Requirement for PCI, NIST 800-53, ISO 27001 etc
  - e.g. VAT (Vulnerability Analysis Tool)

Processors and Partitions

- IODF
- Physical vs Logical
  - Logical Channel Subsystem(s)
  - Logical Partitions
  - Power on Reset
  - I/O Devices
  - IPL
- Living in a Virtual World
- HCD, HCM and HMC
- Don’t call it Legacy!

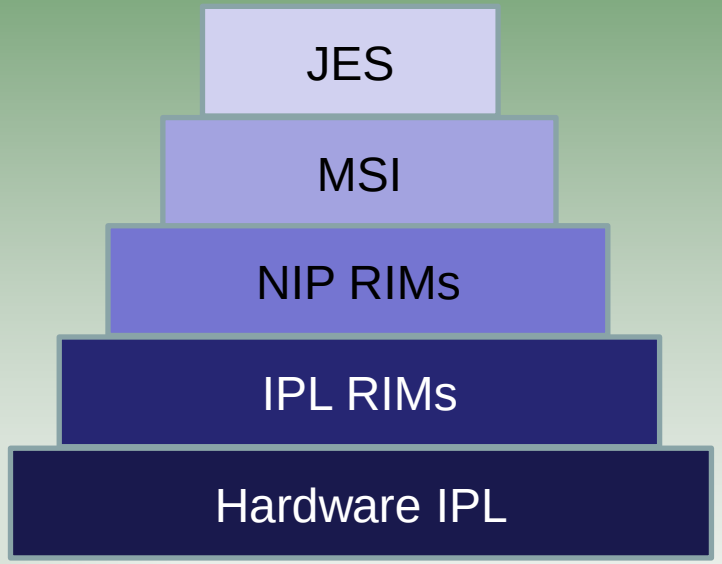
Processors and Partitions

Configuration Drift



IPLing a z/OS Logical Partition

- Process used to initialise z/OS for use
- Similar to PC Boot
  - Hardware
    - IODF
    - Manual
  - Resource Initialisation
  - Nucleus Initialisation
  - Master Scheduler
  - Job Entry
- No security for most of the process!



And Finally...

- The book:
  zAuditing Essentials – Volume 1
  www.newera-help.com/zAudit.html
- The software tool:
  StepOne distributed by NewEra Software Inc
  www.newera-help.com/StepOne-Download.html
- The speaker:
  email: julie@sysprog.co.uk
  mobile: 07770 415102

And Finally...

- Before you go:

IBM 2741 Terminal

- SHARE Security Project
- 1974 Paper – Goals for Security
- To be re-released

Thank You