Diminishing Returns – Audit 101

Colman O'Carroll
Syspertec-Virtel

About Me

- 1991 – 2001
  (z)TPF Assembler Programmer
  UK, USA, Germany & France

- 2002 – Present
  (z)Systems Programmer – *Paris France*

- 2008 – Present
  Technical Trainer – *Anywhere you'll have me ?*

What Have the Romans ever done for us ?

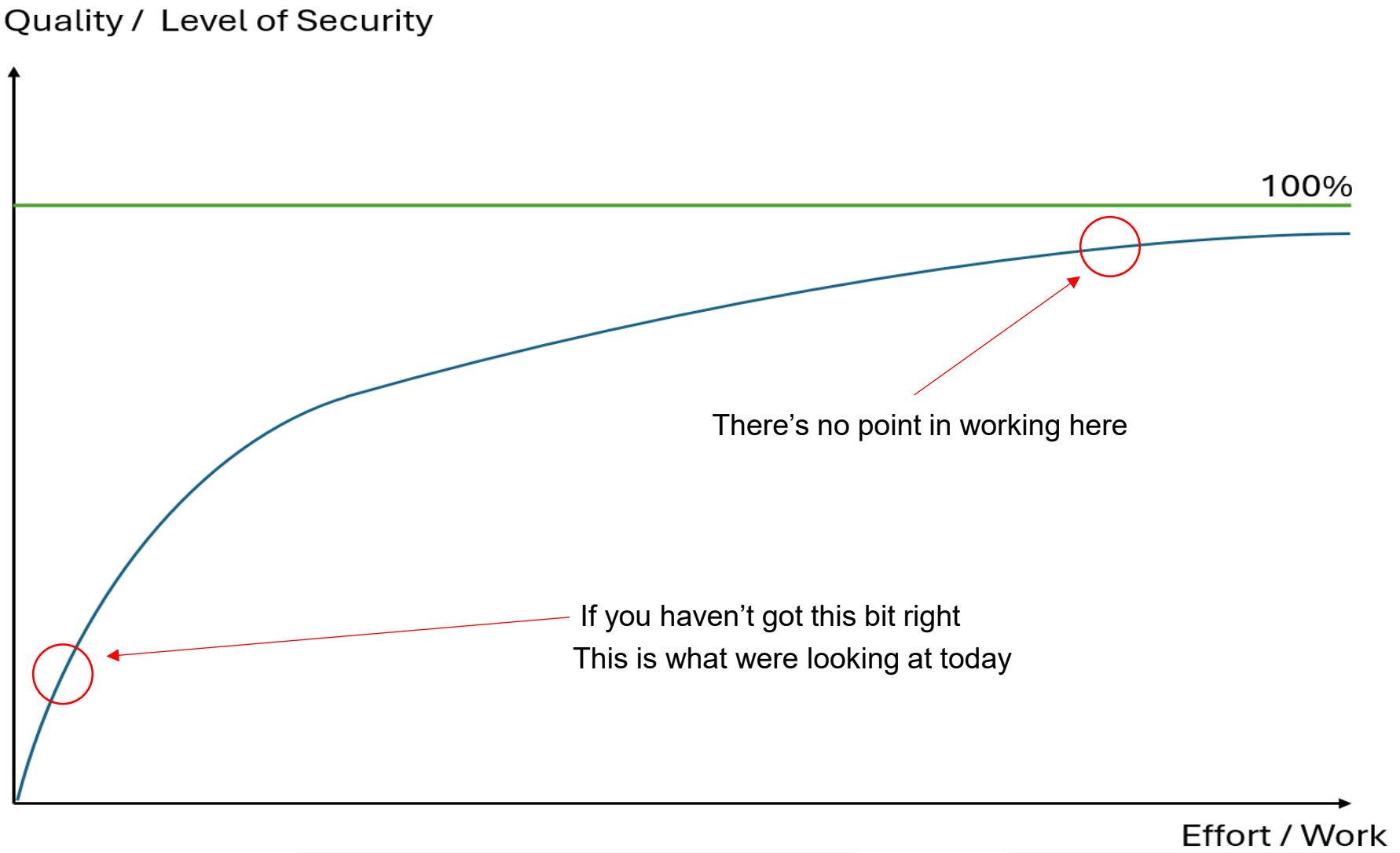
Disclaimer

- All opinions and judgments here are MINE and mine alone.
- Anything I say here is NOT to be taken as any kind of endorsement for a product or service.
- Any kind of “basic audit” cannot be construed as suddenly making your system “secure”.
- If you follow the advice here, you can say that your system is “more secure”
- Most of the details here are RACF influenced but the concepts are universal

Agenda

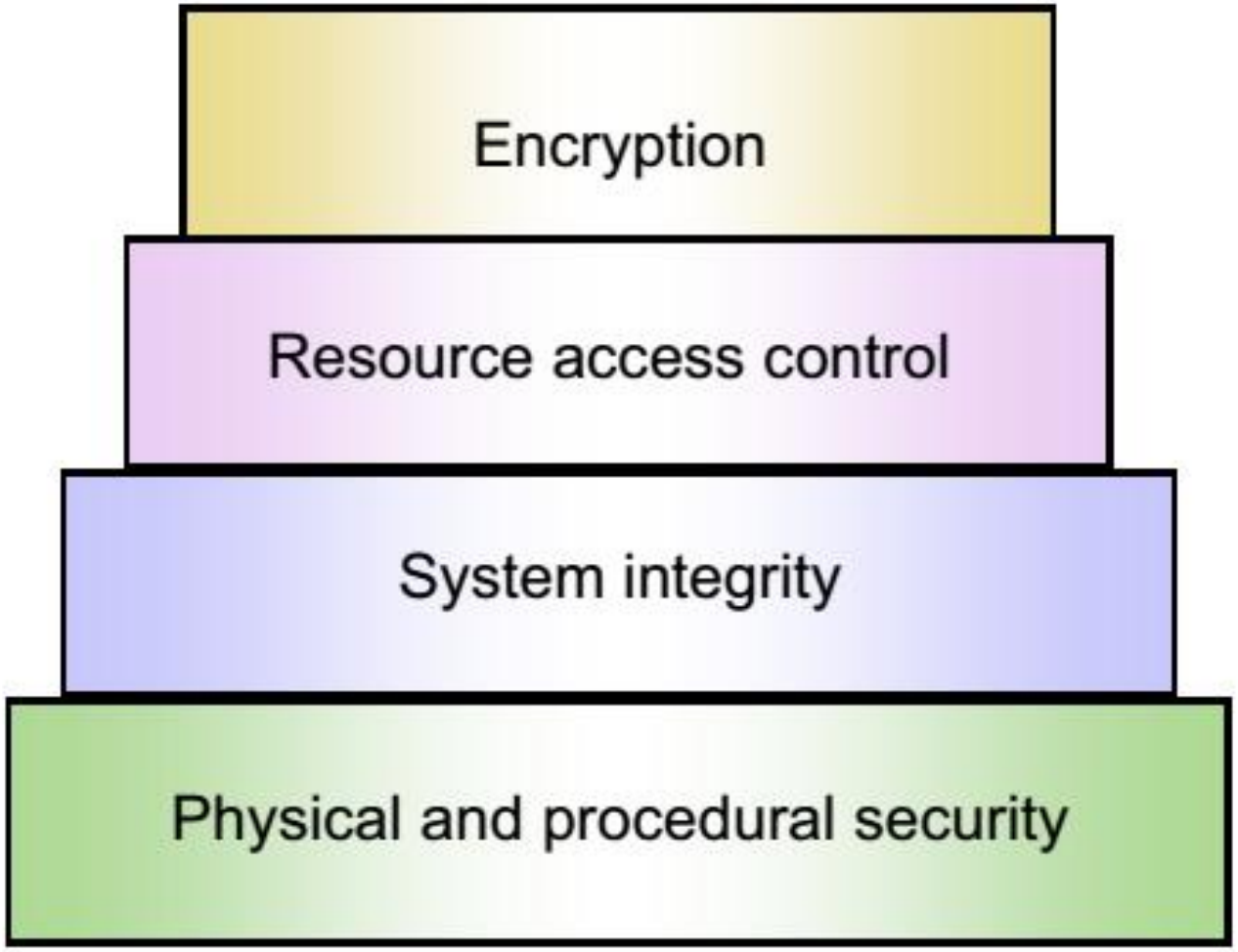
- The “Curve”
  - What it is and trying to evaluate where we are on it.
- Everyone identified?
  - Is it possible ?
- Everything Protected?
  - According to the rules (What are the rules ? ?)
- Everything logged ?
  - Security breaches are a “long game” are you watching everything ALL the time ?
- Everything Encrypted?
  - Up to a point…
- Do you know what your job is ?
  - Roles/Responsibilities

Effort Vs Reward – The notion of diminishing returns



- Small Amount of work
  - High to Reasonable Gain
- Over time Increases become less significant
- 100% is never possible
  - Naïve to assume so

Security Pyramid at a glance.



- At the top of the curve..
  - Is everything else in place ?
- « RAC » The way we look at/consider security in z/OS
- Can you trust what's actually going on in your system.
  - Security is nothing if there are bugs in the code
- Who can actually get the to machines/disk bays

Know YOUR Rules !

- Basic details in your “ISP” or
  - Information Security Policy / Enterprise Policy
- Generalities about:
  - Authentication (Password or strong authentication)
  - Password Length/complexity
  - Expiration/change rules
- Specifics about
  - Data classification
  - Roles & responsibilities
- The mainframe is “different”
  - Do you know/can you interact with the ISP Management to explain and mitigate these differences ?

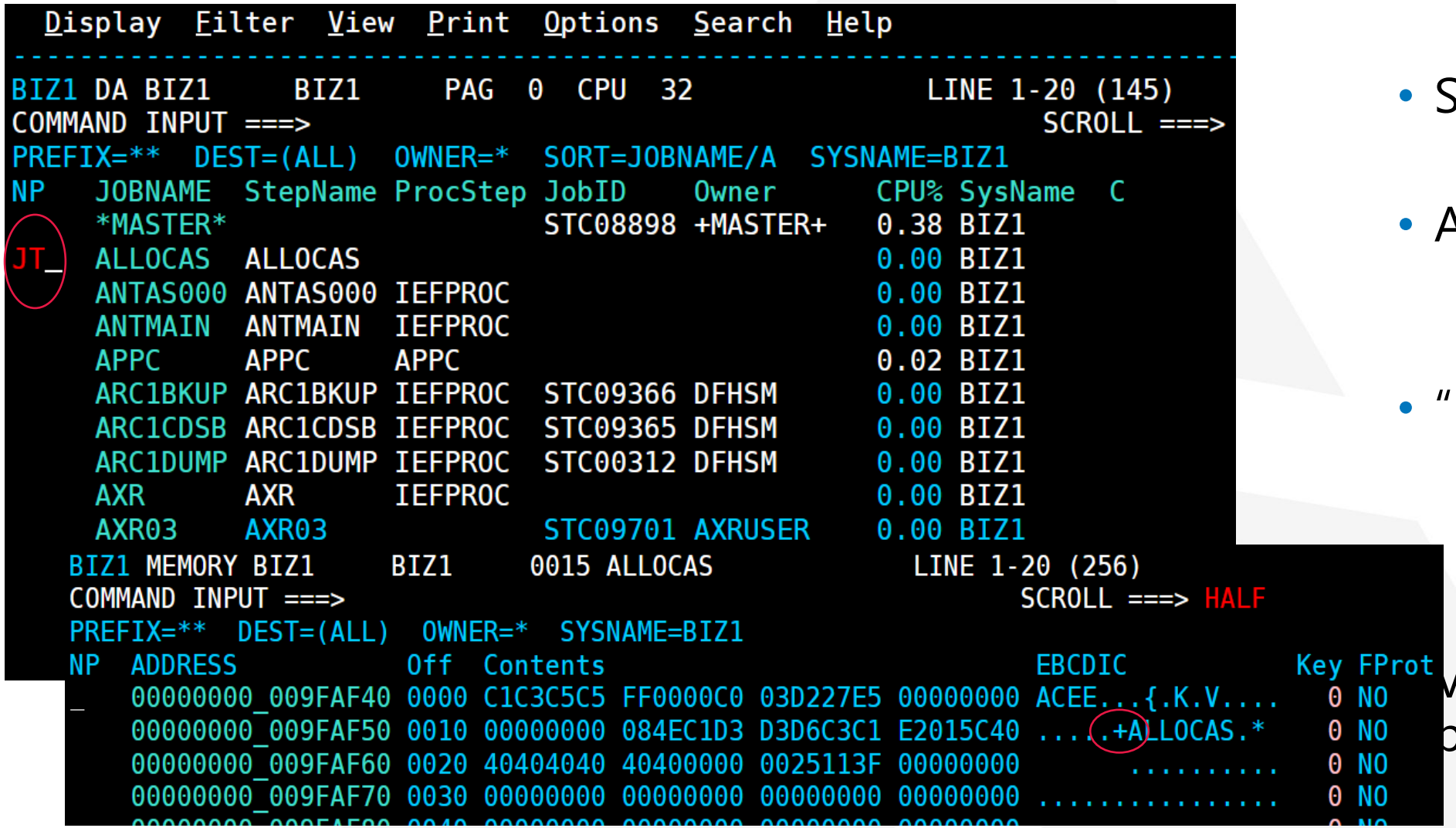
The mainframe differences.

- 8 Character identifier.
  - Architecturally set since the beginning….
  - No plans to change this AFIK
- 8 Character Password
  - Mixed-case and special characters relatively recent.
  - Careful about special characters if you're multi-code-page.
  - Modernisation possible (see later)
- Datasets.. Not files
  - Protection is abstract.
  - In the mainframe, the object protected has no idea of if/how it is managed.
- Oh, and you've got UNIX in there too ;-)

Everybody Identified ?

- Everything that happens in the system must be "loggable" and attributable to a userid/account.
- Human Users
  - Any person who needs to connect to the machine.
  - Either directly (TSO/CICS/IMS) or indirectly (any web service ?)
  - Roles & Responsibilities
- Service Users
  - Schedulers
  - System Automation
- Internal processes (If possible.. ?)
  - CATALOG, IXGLOGR, CONSOLE, WLM ?

System - Userid Visibility



- SDSF DA Panel
  - 'JT' Job Task Command
- ACEE Display
  - New in z/OS 3.1
  - Column on JT Panel
- "+" Indicates default
  - May not be possible to change (today)
  - Integrity/Trust is necessary

Very few system processes concerned.

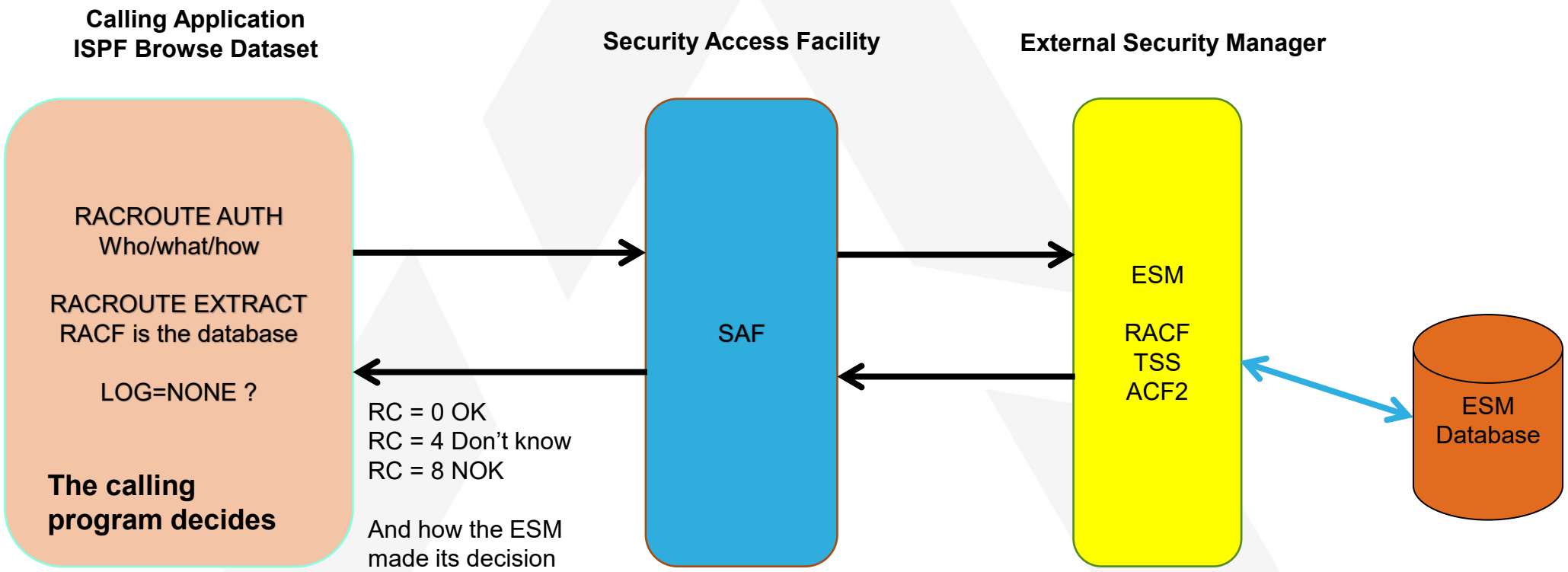
Userids and Password Authentication

- Traditionally 8 characters (7 for TSO) with a 8 Character Password.
  - "FEBR2026" Super ☺
- Many Modern mechanisms to improve this:
  - Passphrases
    - 9 to 100 Characters with built in rules.
  - Multi Factor Authentication
    - Sollicit External site/mechanism for authentication
      - RADIUS/PING/DUO/SECURID etc.
  - Single Signon
    - Kerberos or other external mechanism
    - Userid mapping possible on z/OS
  - Client certificate authentication
    - PKI Infrastructure required
    - Mapping also possible (HostIdMappings 1.3.18.0.2.18.1)
  - Passtickets
    - Used with other authentication mechanisms (single signon, then passticket access to z/OS application)
    - Can be VERY Secure from z/OS to z/OS (with crypto card & HMAC Keys.)

Particular User Attributes

- OPERATIONS
  - Nobody ! Human or otherwise should EVER have this attribute in day-to-day tasks.
  - Even HSM can and should be specifically permitted
  - Privilege escalation MUST be defined and logged correctly
- SPECIAL
  - This is the RACF administrator function.
  - Does NOT give any permissions in and of itself
    - Can give oneself ANY permission.
- AUDITOR
  - Verifies what the RACF Special user does.
  - ROAUDIT
    - New function in RACF.. Who should we give it to ?

How does the ESM work in z/OS, Is everything protected ?



Is Everything Protected ? Data !

- ALL Datasets..
  - RACF PROTECTALL(FAIL) (Or ESM Equivalent)
  - System Critical Datasets (Those that could compromise integrity)
    - SYS1.NUCLEUS/SVCLIB/LPALIB (This code can now be signed.. “Validated boot”)
  - System privileged programs.
    - PPT and LPA
  - User privileged programs
    - The APF List. ! ! !
  - User Data
    - Our actual reason-to-be
    - “Morally” obliged to protect our client data
    - Legally obliged too.; (GDPR)

Is everything protected ? – “Resources”

- ALL system Commands.. (non exhaustive list)
  - ACTIVATE (IODF), CONFIG (paths & processors)
    - Change the system configuration
  - CANCEL, FORCE, MODIFY
    - Could be seriously disruptive
  - SET ! !
    - The “big” one in all its forms.
    - SETPROG, SETSMS, SETOMVS etc etc…
      - AND Don’t forget
    - SET PROG=xx, SET SMS=xx, SET OMVS=xx
- Do we let ordinary users look at stuff ?
  - /D IPLINFO ?
  - /D PROG,APF
  - /D T ?
  - /DEVSERV
  - etc…

Is everything protected ? – IBM Specific mechanisms

- System LOGGER (IXCLOGR)
  - Tampering with the logs could indicate someone trying to hide something.
- BCPii
  - Mostly protected at a H/W HMC Level.
  - A zOS instance with this power can disrupt the whole machine.

Everything logged ?

- It's 03h00 and do you know where your SYSLOGs are ?
- ICH408I and all its variants...
- SMF overview

ICH408I

- The most simple/direct has everything you need
  - USER/GROUP/RESOURCE/CLASS/ASKED/GIVEN + Message

```
ICH408I USER(VTSOCA3 ) GROUP(VIRTUSRS) NAME(COLMAN NON PRIVILEGE)
  SYS2.RACF.BACKUP CL(DATASET ) VOL(BTISY0)
  INSUFFICIENT ACCESS AUTHORITY
  FROM SYS2.RACF.BACKUP (G)
  ACCESS INTENT(READ    )  ACCESS ALLOWED(NONE    )
```

- Many more messages (At least 90 (ninety))
  - DEFINE - INSUFFICIENT AUTHORITY

```
ICH408I USER(VTSOCA3 ) GROUP(VIRTUSRS) NAME(COLMAN NON PRIVILEGE)
  SYS2.RACF.BACKUP.TEST CL(DATASET ) VOL(WRK900)
  DEFINE - INSUFFICIENT AUTHORITY
```

The protecting RACF object is NOT Displayed.

A little digging required.

Access Level Recap

- NONE
  - No access to Resource
- EXECUTE
  - Execute (A program, but NO read (or copy) Access)
- READ
  - Consult
- UPDATE
  - Change the contents
- CONTROL
  - Update for VSAM Control Areas
  - Varies for other resources
- ALTER
  - Create Rename and Delete

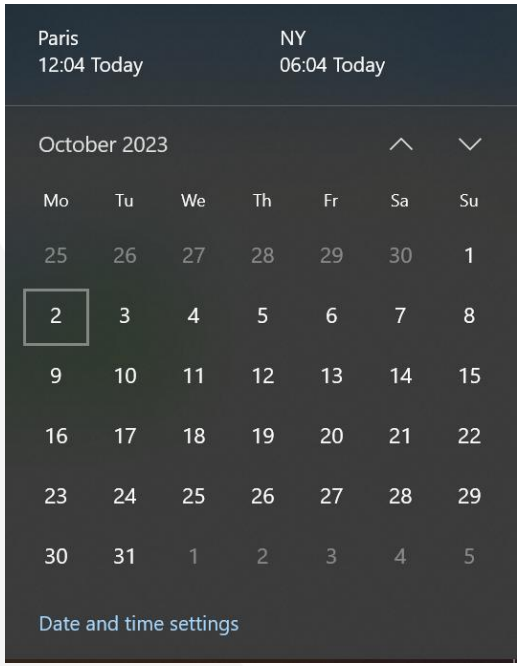
SMF Logging

- MANx Datasets or LOGSTREAMS
  - Traditionally MAN datasets
  - More flexible/modern logstreams available
- All security events should be logged
  - SMF Types:
    - 80 : RACF processing
    - 81 : RACF Initialisation
    - 83 : RACF Audit Record For Data Sets
    - 119 : Network Activity
    - xx : Any other pertinent records (82 for ICSF ?)
  - Make sure SMF Output is NOT “DUMMY”
- SMF Data is :
  - Must/should be signed (higher up on the curve)
  - Post-processed for analysis
  - Can be examined in (near) real-time and sent to an SIEM ? Alerts ?

```
   SYS2.PARMLIB.BTPLEX(SMFPRMPX) - 01.73
===> _____________________________________________________________
SYS(TYPE(7,14,15,17,18,30,37,38,39,42,
         61:69,70:79,80,81,82,83,89,92,114,119,185),
              EXITS(IEFU83,IEFU84,IEFACTRT,
              IEFUSI,IEFUJI),NOINTERVAL,NODETAIL)
```

Where are the Logs ?

- z/OS SYSLOG/OPERLOG ?
  - SDSF/Sysview/Console
- syslogd – standard unix system logging
- trmd - traffic regulation manager
- Not always necessary (ipsec/ids/zert)
- sshd - OpenSSH daemon
- Attention: - Save yourself a lot of heartache; get the timestamps correct !
- TZ=CST-1CEST,M3.5.0,M10.5.0 ? ? ?



Everything Encrypted ?

- Traffic into and out of z/OS
  - Its 2026, anything leaving or entering the z/OS System needs to be encrypted. (The “most secure possible” SSL/TLS Mechanisms)
  - TLS1.2 Minimum. TLS 1.3 better.
  - Many IBM “out of the box” tools to check this.
  - Don’t Forget VTAM
- Data at rest.
  - Modern Disk bays can and should already be encrypted (invisible to z/OS)
  - Pervasive encryption
    - Higher on the curve, priority 1 after the basics..
- RAM Encryption ?
  - z/16 Transparent memory Encryption

Everyone knows their role/responsibility ?

- Correct process for changes
  - provisioning/de provisioning.
  - Software Installation
  - System Upgrades
  - Emergencies ?
    - Watch out for holes… Too easy to break glass.. Or non-expiring passwords.
- What's your decisional mandate when there's a problem ?
  - There are MANY ways to "fix" a problem
    - Specific Dataset permissions Vs "Operations"
  - Usage of the new ROAUDIT Attribute
  - What to do when something goes wrong ?

Conclusion

- Don’t Panic
- Know your rules
- Everybody Identified
- Everything protected
- Everything logged
- Everything Encrypted
- Everyone knows their job ?

- Thanks for listening.

Your feedback is important!

SHARE
EDUCATE • NETWORK • INFLUENCE

Submit a session evaluation for each session you attend:

www.share.org/evaluation