SHARE
EDUCATE • NETWORK • INFLUENCE

10 Legacy Decisions That Are Security Risks Today

Kevin Segreti
Client Services Technical Consultant
kevin.segreti@broadcom.com

Carla Flores
Cybersecurity Solution Advisor
carla.flores@broadcom.com

Disclaimer

Certain information in this presentation may outline Broadcom's general product direction. This presentation shall not serve to (i) affect the rights and/or obligations of Broadcom or its licensees under any existing or future license agreement or services agreement relating to any Broadcom software product; or (ii) amend any product documentation or specifications for any Broadcom software product. This presentation is based on current information and resource allocations as of August 4, 2026, and is **subject to change or withdrawal by Broadcom at any time without notice**. **The development, release and timing of any features or functionality described in this presentation remain at Broadcom's sole discretion**.

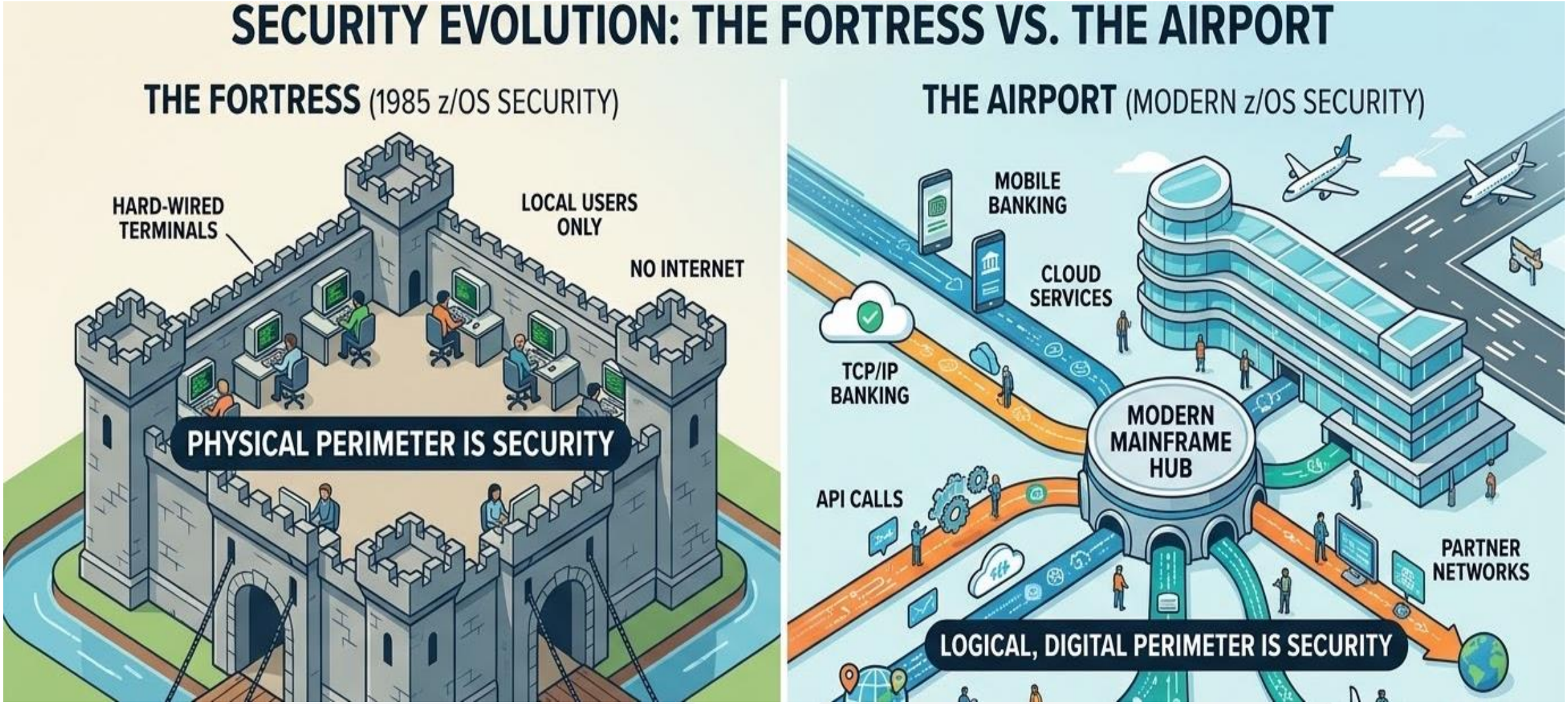
Notwithstanding anything in this presentation to the contrary, upon the general availability of any future Broadcom product release referenced in this presentation, Broadcom may make such release available to new licensees in the form of a regularly scheduled major product release. Such release may be made available to licensees of the product who are active subscribers to Broadcom maintenance and support, on a when and if-available basis. The information in this presentation is not deemed to be incorporated into any contract.

Broadcom may use any feedback provided by you related to a Broadcom product or this presentation for any Broadcom business purposes (including but not limited to, preparation, reproduction, and distribution of derivative works based upon such feedback), without any obligation to you including consent or payment.

THIS PRESENTATION IS FOR YOUR INFORMATIONAL PURPOSES ONLY. Broadcom assumes no responsibility for the accuracy or completeness of the information. TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON INFRINGEMENT. In no event will Broadcom be liable for any loss or damage, direct or indirect, in connection with this presentation, including, without limitation, lost profits, lost investment, business interruption, goodwill, or lost data, even if Broadcom is expressly advised in advance of the possibility of such damages.

The Shift in Security Phlosiphy

SHARE
EDUCATE • NETWORK • INFLUENCE



The Hidden Debt of "It Just Works"

SHARE
EDUCATE • NETWORK • INFLUENCE

The Reality of 2026:

- **The Internet Factor:** Decisions made in the 1980s assumed a "walled garden." Today, the mainframe is a connected hub, making legacy circumventions (like NON-CNCL or BYPASS) high-velocity risks.
- **The Complexity Tax:** Decades of "temporary" access grants and broad organizational ‘global access’ have created a security surface area that is difficult to audit and near impossible to defend.
- **Compliance Pressures:** Modern frameworks (DORA, PCI-DSS 4.0, NIST) no longer accept "standard practice" as a valid excuse for over-privileged accounts.

Our Objective:

- **Identify:** Pinpoint some of the most common "legacy ghosts" haunting our ACF2 and Top Secret databases.
- **Analyze:** Use modern Auditing and Reporting (ACFRPTRV/TSSUTIL) to measure the gap between *current* access and *actual* need.
- **Remediate:** Transition from "Wide Open” to a **Least Privileged Model** without disrupting the business.

Removing SAF Bypass Authority

BYPASS Authority in Top Secret

SHARE
EDUCATE • NETWORK • INFLUENCE

Bypass Attributes aka "**NO NO**" Bits

NODSNCHK: Bypasses all Data Set security validation; allows Read, Write, or Delete for any file.

NOVOLCHK: Bypasses Volume-level security checking for direct Disk or Tape access.

NOSUBCHK: Bypasses Job Submission validation; allows submitting JCL as any ACID.

NOLCFCHK: Bypasses Limited Command Facility checks for TSO, CICS, and IMS commands.

NORESCHK: Bypasses security for Abstract Resources (non-dataset/non-volume classes) in the RDT.

NOVMDCHK: Bypasses VM Minidisk link checking (primarily used in z/VM environments).

Started Task Table

Kevin's Method of Remediation

1. Grant WARN MODE to the ACID and remove the Bypass Attributes in Question.

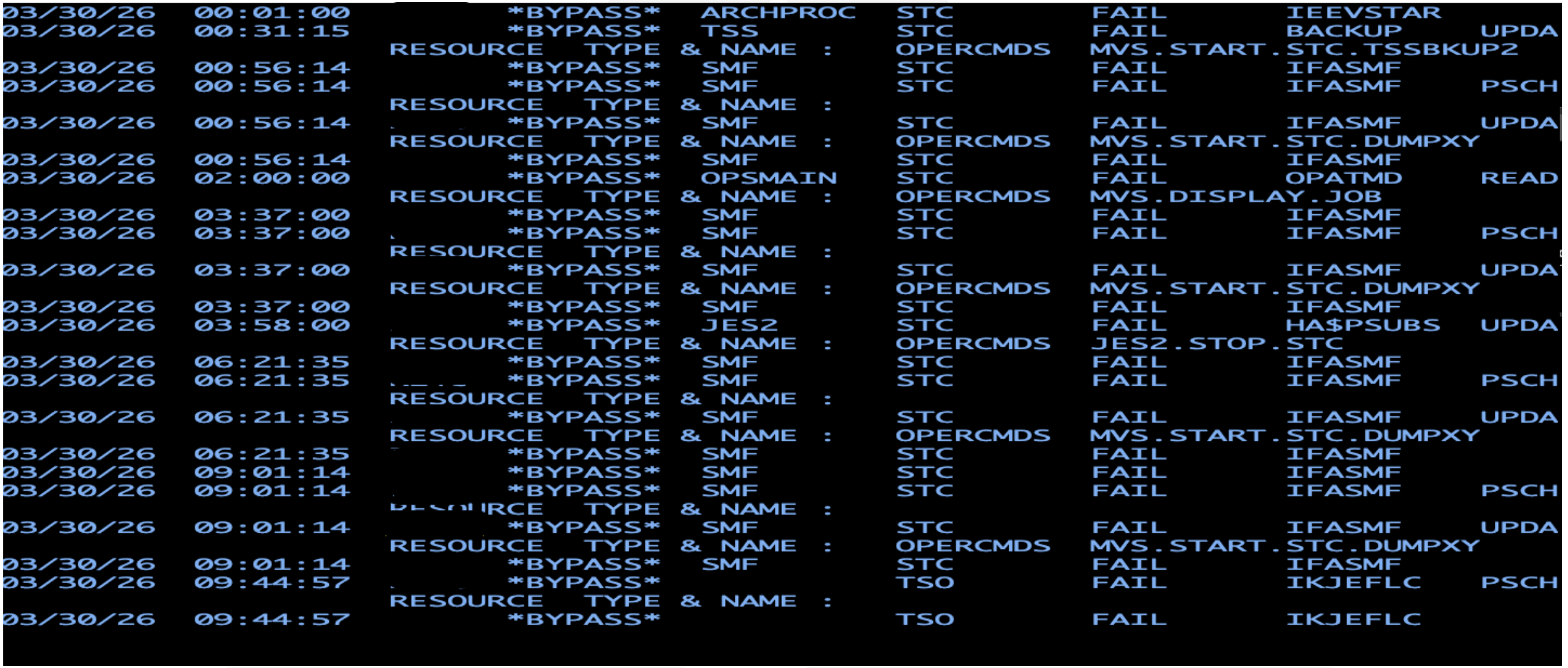
   TSS PERMIT(acid) MODE(WARN) FOR(180)
   TSS REMOVE(acid) NODSNCHK NOVOLCHK NOSUBCHK
   NORESCHK NOLCFCHK

   TSS ADD(STC) PROCNAME(stc) ACID(acid)

```
//REPORTS          EXEC        TSSUTILA
//TSSIN            DD          *
REPORT EVENT(VIOL) MODE(WARN) DATE(-01)
LONG END
/*
```

2. Audit the use of WARN mode for the ACID in Question.

Top Secret TSSUTIL Records EVENT(AUDTB)



```
03/30/26   00:01:00          *BYPASS*   ARCHPROC   STC          FAIL         IEEVSTAR
03/30/26   00:31:15          *BYPASS*   TSS        STC          FAIL         BACKUP      UPDA
                     RESOURCE   TYPE  & NAME  :   OPERCMDS    MVS.START.STC.TSSBKUP2
03/30/26   00:56:14          *BYPASS*   SMF        STC          FAIL         IFASMF
03/30/26   00:56:14          *BYPASS*   SMF        STC          FAIL         IFASMF      PSCH
                     RESOURCE   TYPE  & NAME  :
03/30/26   00:56:14          *BYPASS*   SMF        STC          FAIL         IFASMF      UPDA
                     RESOURCE   TYPE  & NAME  :   OPERCMDS    MVS.START.STC.DUMPXY
03/30/26   00:56:14          *BYPASS*   SMF        STC          FAIL         IFASMF
03/30/26   02:00:00          *BYPASS*   OPSMAIN    STC          FAIL         OPATMD      READ
                     RESOURCE   TYPE  & NAME  :   OPERCMDS    MVS.DISPLAY.JOB
03/30/26   03:37:00          *BYPASS*   SMF        STC          FAIL         IFASMF
03/30/26   03:37:00          *BYPASS*   SMF        STC          FAIL         IFASMF      PSCH
                     RESOURCE   TYPE  & NAME  :
03/30/26   03:37:00          *BYPASS*   SMF        STC          FAIL         IFASMF      UPDA
                     RESOURCE   TYPE  & NAME  :   OPERCMDS    MVS.START.STC.DUMPXY
03/30/26   03:37:00          *BYPASS*   SMF        STC          FAIL         IFASMF
03/30/26   03:58:00          *BYPASS*   JES2       STC          FAIL         HA$PSUBS    UPDA
                     RESOURCE   TYPE  & NAME  :   OPERCMDS    JES2.STOP.STC
03/30/26   06:21:35          *BYPASS*   SMF        STC          FAIL         IFASMF
03/30/26   06:21:35          *BYPASS*   SMF        STC          FAIL         IFASMF      PSCH
                     RESOURCE   TYPE  & NAME  :
03/30/26   06:21:35          *BYPASS*   SMF        STC          FAIL         IFASMF      UPDA
                     RESOURCE   TYPE  & NAME  :   OPERCMDS    MVS.START.STC.DUMPXY
03/30/26   06:21:35          *BYPASS*   SMF        STC          FAIL         IFASMF
03/30/26   09:01:14          *BYPASS*   SMF        STC          FAIL         IFASMF
03/30/26   09:01:14          *BYPASS*   SMF        STC          FAIL         IFASMF      PSCH
                     RESOURCE   TYPE  & NAME  :
03/30/26   09:01:14          *BYPASS*   SMF        STC          FAIL         IFASMF      UPDA
                     RESOURCE   TYPE  & NAME  :   OPERCMDS    MVS.START.STC.DUMPXY
03/30/26   09:01:14          *BYPASS*   SMF        STC          FAIL         IFASMF
03/30/26   09:44:57          *BYPASS*              TSO          FAIL         IKJEFLC     PSCH
                     RESOURCE   TYPE  & NAME  :
03/30/26   09:44:57          *BYPASS*              TSO          FAIL         IKJEFLC
```

Access Circumvention in ACF2

- LID privileges:
  - SECURITY: Allows update access to the ACF2 security databases + access to ALL datasets, protected programs, and resources
  - READALL: Allows READ and EXECUTE access to ALL DATASETS
  - NON-CNCL: Allows ALL access to ALL datasets and resources

- SAFDEF=GSO with MODE=IGNORE:

```
DFDSS     JOBNAME=********   USERID=********   PROGRAM=ADR*****   RB=ADR*****
          RETCODE=0          SAFDEF=GSO        MODE=IGNORE        SUBSYS=****
          FUNCRET=4          FUNCRSN=0

          RACROUTE REQUEST=AUTH,CLASS='DATASET'
```

Access Circumvention in ACF2

- PREFIX on LID record: Specifying a key in the PREFIX field indicates that the user owns that key and automatically has access to that data.
  - $PREFIX in lid record can be set to anything and/or masked
    - Default should match the LID, but it can be changed (ie. $PREFIX(PROD****)

- MAINT RECORDS:

  Full access to the program in the matching library by the LID specified. *(Note: the LID must have the MAINT privilege as well)*

```
-- MAINTENANCE LOGONIDS/PROGRAMS/LIBRARIES --
 LIDTEST  ADRDSSU  SYS1.LINKLIB
 LIDTEST  ARCCTL   SYS1.LINKLIB
 LIDTEST  CTDSDUMP SYS1.LINKLIB
 LIDTEST  DGTFDS00 SYS1.LINKLIB
```

- EXITS should be reviewed and documented.
  - Any that circumvent normal ACF2 processing should be monitored for changes.

Carla's Method of Remediation

- ACF2 logs any accesses the user makes that are not allowed through ownership or through dataset and resource rules (NON-CNCL, SECURITY, READALL, etc).
- Review the ACFRPTDS and ACFRPTRV reports for any logging messages and write the appropriate rules for access.

```
SYSVIEW  26.056 02/25 00.00      DATASET  LOGGING   NON-CANC
SYSVUSR  VOL=       DDN=          DSN=SYSPDATA.SYSVIEW.CAP.T0000173.D260225
SYSVUSER VOL=LLA001 PGM=GSVXASCT LIB=SYS3.SYSVIEW.R17L.CNM4BLOD
STC24805 ALLOC  ALLOC   NORECORD NAM=SYSVIEW STC ID       ROL=
OPS  SAF SRC=STCINRDR            UID=SYSVIEW
```

- Keep reviewing the report(s) until no records show up.

Enabling AES-256 Bit Encryption in ACF2 and Top Secret

The Need for AES256 Bit Encryption

Introduction to AES256 Security in ACF2

- ACF2 supports both AES128 and AES256 encryption.
- ACF2 continues to supports XDES while it is not recommended encryption method to be used now.
- AES256 encryption can be easily enabled/activated through ACF2 Global system options (GSO).
- GSO PSWDOPTS record has PSWDENCT which controls how passwords and password phrases are encrypted and stored. PSWDENCT(AES2) will enable AES256 encryption

How to Encryption Settings in ACF2

- Issue the **SHOW PSWD** command - you will see all the password options in effect and look for:

```
OPTION                          OPTION DESCRIPTION
=================================================
PSWDENCT = AES2          PWSD ENCRYPTION ALGORITHM UTILIZED
```

** AES2 is AES256

*** It will display AES if AES128 or DES.

Implementing AES256 in ACF2

Prerequisite Steps:

- Ensure that your site has the latest maintenance for AES256 support applied.
- Ensure you have a separate backup of all ACF2 security database. (F ACF2,BACKUP)

Implementation Steps:

- Set PSWDENCT(AES2) in the GSO PSWD record
- Ensure you have a separate backup of all ACF2 security database. (F ACF2,BACKUP)
- Set NOONEPWALG in the GSO PSWD record. NOONEPWALG saves password changes under multiple algorithms.
- Set the PSWD-EXP field on the logonid to manually expire password. This will require user to change password/phrases.
- If a password change is not possible due to static passwords, then change logon id to have PWCNVRT. This is an additional ability to do the encryption without needing to change password
- Define the ONEPWALG field of the GSO PSWD record once all passwords have been successfully changed or converted
- Run the ACFRPTSL report to validate single AES256 algorithm usage

https://techdocs.broadcom.com/us/en/ca-mainframe-software/security/ca-acf2-for-z-os/17-0/administrating/implement-aes-256-encryption.html

Introduction to AES256 Security in TSS

- Top Secret supports both AES128E and AES256 encryption
- Top Secret continues to support XDES but it is not recommended to be used
- AES256 is more secure than Triple-DES and AES128(E)
- 256 bit key size increases security due to the number of possible key combinations
- Performance improvement with AESCACHE option
  - Enabled by default with AES256
  - Encryption of password/phrase is done one time then stored in cache
  - Cache can be cleared or users are removed over time
- Converting from AES128(E) to AES256 can be activated by the control option AESENC(256).

How to Encryption Settings in TSS

- Issue the **TSS MODI STATUS** command - you will see the following section:

```
TSS9661I          Top Secret FEATURES Status
MAX_ACID_SIZE(2048K)
ORG_ACID_SIZE(2048K)
AES_ENCRYPTION(Active,256)
LARGE_VSAM_RECORD(0034K)
EXPAND_COUNTER(Active)
```

** Active,256 is AES256

*** It will display (Active, AES128) if AES128, or (Active,AES128E) if AES128E, or **nothing will display** if it is DES

Converting TSS File for AES256

- Converting from XDES to AES 256 requires a security file conversion
  - The backup security file is used for conversion
  - Run TSSMAINT to create new security files (SECFILE, VSAMFILE, etc)
    - AES256ENCRYPT option in parameter file
  - Run TSSEXTEND to copy the backup security file and convert passwords to AES 256
- Converting from AES 128(E) to AES 256 does not require security file conversion
  - Change control parameter AESENC from AESENC(128) or AESENC(128E) to AESENC(256)
  - As passwords are changed, they will be encrypted with AES256
  - If converting from AES128, the security file conversion can be run to convert all passwords to AES 256
  - If converting from AES128E, just the control parameter can be changed. Or security file conversion can be run.
  - Using the AESENC control option will only encrypt new passwords going forward with the new level of encryption.

https://techdocs.broadcom.com/us/en/ca-mainframe-software/security/ca-top-secret-for-z-os/17-0/administrating/managing-passwords-and-password-phrases/implement-256-bit-aes-encryption-for-passwords-and-password-phrases.html

Remediate the use of NOPW in Top Secret

Ensuring Zero Trust with password and passphrase in TSS

History: Top Secret can create User IDs with no password assigned to them. When a user ID is created with no password, any password value is allowed to authenticate the user. In the past this value was needed for Started Tasks so they would not produce a console request requiring the password to be entered. It is no longer necessary for Started Tasks to produce console requests for password, which has depreciated the need for this password value.

Description: With no password being assigned to a User ID, only Facility access is required to sign on to the system.

Remediation Steps: All active IDs on the list should be either converted to PROTECED User IDs or should be give a proper password. Detailed descriptions of the steps can be found in STIG BTSS0005.

Ensuring Zero Trust with password and passphrase in TSS

- Top Secret introduced a new control option NOPW with PTFs **LU15394, LU16786, and LU17521**
  - This control option is designed to help you migrate from Warn to Fail
  - The NOPW control option is not valid in V17 of Top Secret and has been removed.
  - TSSUTIL can be used to Audit the use of NOPW
- Top Secret has a NOPW counter in V16 to monitor usage

TSS MODIFY STATS

```
TSS9590I Init(000000940) Xreq(000003437)  Mvs(000088327)
TSS9591I Viol(000000243) Exec(000001514)  Smf(000088277)
TSS9592I Chng(000000015) Recv(000000265)  Aud(000088295)
TSS9593I Read(000026272) Writ(000002229)  Hwm(000000010)
TSS9594I #Req(000000000) Lock(000000001)  Lwt(000000000)
TSS9595I Mwrt(000002227) NPWS(000000005)
. . .
```

No More Passwords!

Passwords and Passphrases

Foundational differences

RACROUTE Parameter:
- Password = PASSWRD or NEWPASS
- Passphrase = PHRASE or NEWPHRASE

Character length:
- Passwords = 1-8 characters
- Passphrases = 9-100 characters

Database field:
- ACF2 = PSWD Record, ALLOW/PWPALLOW
- Top Secret = PASSWORD, PSWDPHRASE

Enforcement and management

Login
- If a user has both, either valid credential works

Policies
- Password history – NIST guidance is preventing the last 5 historical iterations
- Interval – Compliance frameworks vary
- Length – 15 characters suggested
- Complexity – character type, case type, repeating characters, reserved words, sequential characters, etc
- Failed attempt criteria – Compliance framework vary

Configuring ACF2 with Passphrase

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

Setting a user's passphrase - PWPHRASE User Profile Records

The PWPHRASE USER profile record is used to retain user password phrase control information and history. These records are in the INFOSTG database and are not part of the logonid record.

PWP-EXP|NOPWP-EXP
PWP-HST(0|nn) **
PWP-MAXD(0|nnn)
PWP-MIND(0|nnn)
PWP-TOD(date) **
PWPA1TOD(date) **
PWPA2TOD(date) **
PWPHRASE(password phrase)

Fields marked ** are managed internally by ACF2 and cannot be modified by the ACF command.

When implementing Password Phrase, an administrator must set the user's first Password Phrase. From that point moving forward the end users can change their password phrase. The only other option is for the end user to set their own first Password Phrase using the TSO ACF command processor (if allowed).

Configuring TSS with Passphrase

On the Top Secret side:

- The first thing to do is TSS MODIFY and make sure that NEW_PASSWORD(Active) is shown in the output.

- The next thing to do is set up the passphrase related control options based on your security policy requirements. For example:

NEWPHRASE(MIN=9,MAX=14,WARN=03,MINDAYS=03,NR=3,SC=00,MA=00,MN=03)
NPPTHRESH(5)
PPEXP(060)
PPHIST(12)
PSWDPHRASE(ON)

NOTE: If PSWDPHRASE(OFF) is set, users must have the PSWDPHR attribute set to specify a password phrase.

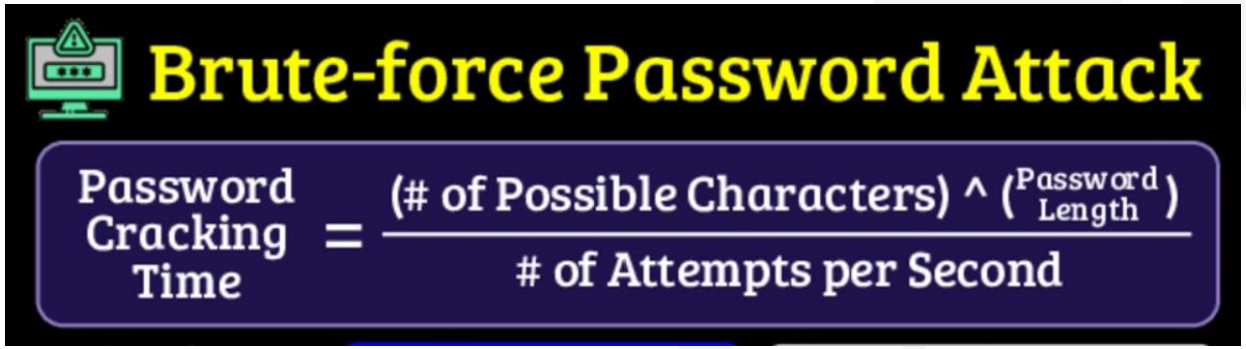
The above are just examples. The control options should be set to your site's standards.

- If the ACID does not already have a passphrase, add a phrase and expire it to force the user to change it. For example:

TSS ADD(acid) PHRASE(thisisthepassphrase,nnn,EXP)

where 'nnn' is the expiration interval for the passphrase.

Even Better!
Look to Deploy MFA Across the Mainframe



Turning MFA on prevents
99%
of cyber attacks that compromise accounts.

A digital identity cannot be trusted when only one factor is used for authentication

- Multiple factors are required for authentication
- Regulatory compliance to PCI DSS, NIST SP 800, HIPAA, Federal Executive Order, ISO 27001, GDPR, plus more
- Built in resilience: 'password fallback' access for designated identities
- Significant reduction in fraud and data breaches!

Authentication Recommendations

SHARE
EDUCATE • NETWORK • INFLUENCE

MFA

- Human & Non-human IDS
- Best choice for interactive Human IDs
- Not viable for most non-human IDs (batch, services, STCs etc.)
- Most secure for interactive IDs

Enhanced Pass Tickets

- Human & Non-human IDs
- Best choice for Non-human IDs
- Reduces the burden of rotation and are generally more secure
- Requires strong protection and lifecycle management of SSIGNON keys and PTKTDATA records
- This strategy avoids storing passwords / passphrases in scripts, JCL, or config files

Passphrase

- Human & Non-human IDs
- May be only viable option for non-human IDs if system times are not in synchronized.
- More secure than PASSWORD
- Note: A Passphrase being used programmatically has to be stored *somewhere*, which opens the credential up to potential exposure

Password

Primarily Human

Primarily non-human, can be used for humans in SSO flows

Both human and non-human - discouraged for non-human where programmatic storage is required.

Password: discouraged for both; transitional only

Remediate the use of UID(0)

The Overuse of UID(0)

SHARE
EDUCATE • NETWORK • INFLUENCE

The Historical "Easy Button”

- **The Trend:** In the 1990s and 2000s, UID 0 was frequently granted to developers, system programmers, and started tasks to bypass complex HFS/ZFS permission bit settings.
- **The Rationale:** It was seen as an administrative shortcut to avoid production delays and "Permission Denied" errors in the shell.

The Reality: Who *Actually* Needs It?

- In a modern, secure z/OS environment, only a handful of specific system functions truly require UID 0.
- Most others should use **UNIXPRIV** class profiles instead.

The "Legitimate" use of UID(0)

Category	Specific ID / Process	Technical Necessity
The Kernel	**OMVS / BPXAS**	Orchestrates all Unix services; requires absolute authority to manage address spaces.
Security	**Started Task (RACF/TSS/ACF2)**	Must be able to switch security environments (ACEEs) and override all file permissions.
Communication	**TCPIP / CSIVPN**	Needs UID 0 to bind to "privileged ports" (below 1024) and manage the network stack.
System Init	**/etc/rc**	The initialization shell script that starts all other daemons at IPL.
Vital Daemons	**syslogd / snmpd**	Requires global access to write logs and monitor system-wide resources.

Remove Unused IDs and Entitlements in your Environment

A Real-World Case Study

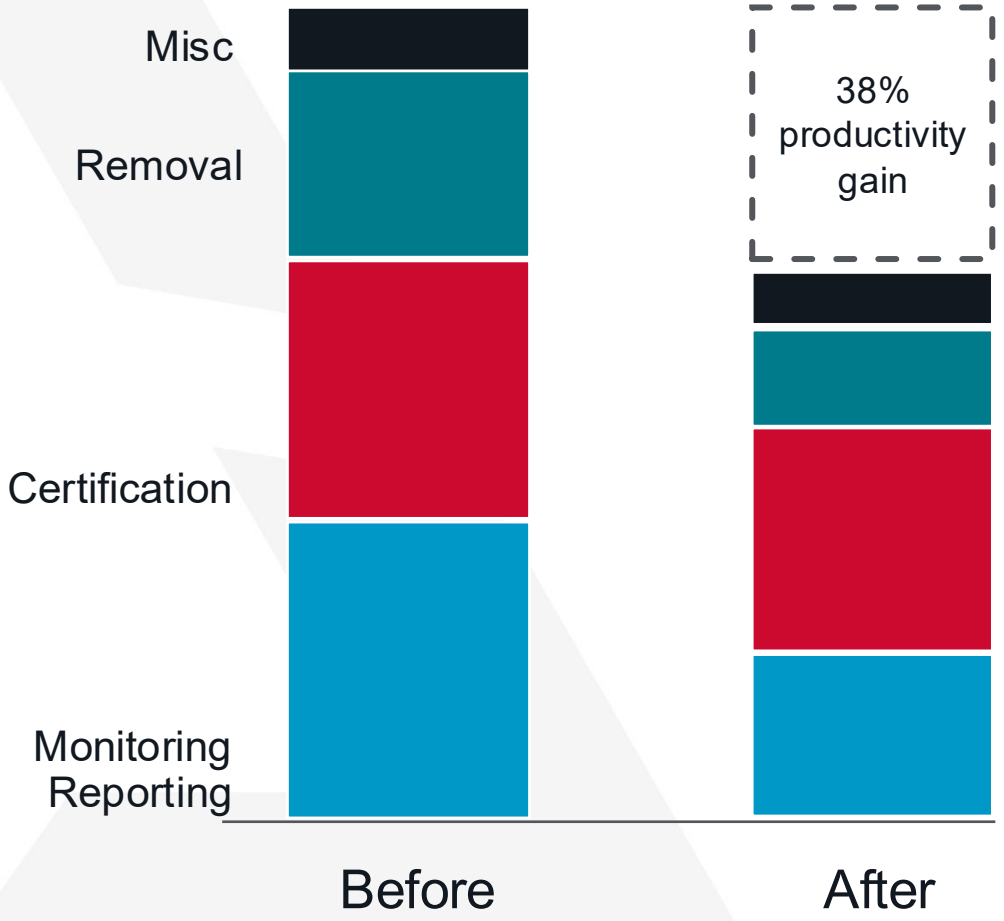
Investment

A security practitioner will take an estimated 5 minutes per user and 15 minutes per access permission (conservative figure).

Average of 20,000 users and 60,000 entitlements per LPAR.

Returned

Savings of 2,400+ engineer hours per year



‘Cleanup’ with ACF2 and TSS

- **ACF**RULCU – ACF2 utility that will identify all dataset and resource rules where a LID or UID string exists, but that LID or UID string no longer exists in the ACF2 database
- **ACF**XREF – ACF2 utility that will identify where a LID exists in an XREF record that no longer exists on the ACF2 database.

- **TSS**: Deleting a user acid cleanly removes it from all profiles and groups connected
  - IF the ACID is an owner of a resource that has been permitted out TSS will not let the delete command work
  - Consideration: Empty Profiles and Groups where no users are attached to them you have to manually list the TSS database to find them

More ‘cleanup’ with tooling

There are several products out there that go beyond what ACF2, TSS or even RACF can do natively related to housekeeping.

Key Features to Consider:

- **Realtime Usage Monitoring**: Cleanup interfaces with your ESM and SAF environment to identify which database entries were used to satisfy a SAF request.
- **Automated Cleanup:** Reduces manual intervention by automating the removal of unnecessary users, entitlements, roles, profiles, and groups
- **Easy Recovery:** Cleanup automatically generates commands to restore any security elements deleted during the cleanup process.
- **Phased Approach:** Cleanup allows you to select what to clean up. You can start with small campaigns and gradually expand your cleanup activities as you gain confidence in the process

Evaluate Global Access Rules

Top Secret ALL Record

- The Top Secret ALL Record is what every ACID created on the system will have access to if no other permissions or profiles are on the ACID.
- The AUTH setting in Top Secret controls the order the ALL record is searched.
  - Options are OVERRIDE, ALLOVER MERGE,ALLOVER MERGE,ALLMERGE

Document what you have in the ALL Record with an explanation of why they are there!

- Things to avoid in your ALL record:
  - Facility Entitlements
  - Access None Rules
  - Entitlements at the HLQ level ex. SYS1
- Appropriate entries for the ALL record
  - Access to your own HLQ
  - Access to your own temporary datasets
  - A VOLUME(*ALL((G)) ACCESS(CREATE) permission

ACF2 “Global Access”

- Historical “Easy Button”
- **IN** rules:
  - Dataset Rules: - UID(*) R(A) W(A) A(A) E(A) or even R(L) W(L) A(L) E(L)
  - Resource Rules: UID(*) ALLOW or UID(*) LOG

- **AS** a resource rule:
  - $KEY(********) TYPE(SAF)*
    UID(*) ALLOW
  - $KEY(**********) TYPE(SAF)*
    UID(*) ALLOW

** Could be any resource type!*

Document the rules you have as Global Permission with an explanation of why they are there!

Fun fact: use $USERDATA in the rule itself or DATA on the rule line and the documentation lives with the rule!

Stop using $VS in Batch

The "Invisible JCL" Risk

The primary danger of using $VS is that it processes the input stream as a raw command. If the file you are pointing to contains multiple JOB cards or interleaved JCL, the system may execute parts of that file that the user didn't intend to run.

Batching Errors: A single file might contain a "test" job followed by a "production" job. If a user uses $VS thinking they are only running the first block, the system may ingest the entire stream.

Hidden Jobs: Because $VS is often used to "punch" or "read" a member into the internal reader (INTRDR), it can trigger every job defined in that member simultaneously.

Identity Hijacking & Authority Issues

In a standard JCL submission (via TSO/ISPF or FTP), the security exit of the **Internal Reader** validates the user's credentials. However, $VS operates at a system command level, which complicates the audit trail.

Credential Masking: If a user with high-level authority (like an Operator or SysProg) uses $VS to submit a file owned by someone else, the jobs within that file might execute under the security context of the **USER=** parameter on the JCL card rather than the person who physically hit "Enter."

Lack of Attribution: If a malicious job is submitted via $VS, the SMF (System Management Facilities) records may show the submission source as a system console or a started task rather than a specific TSO ID, making forensic analysis much harder.

Bypassing Modern Governance

Standard JCL submission usually goes through a **JCL Manager** or a **Scheduling System** (like Control-M or IWS). These tools provide:

- **Syntax Checking:** Ensuring the JCL won't crash the initiator.
- **Change Control:** Ensuring only approved versions of JCL are run.
- **Security Scanning:** Checking for unauthorized DSP=OLD on sensitive datasets.

Using $VS bypasses these filters entirely. It is the mainframe equivalent of running a script as "Root" without checking what the script actually contains.

Make sure you are creating Proper Audit Records

Audit Records

*By default, both ACF2 and Top Secret are configured to only log access attempts that are **denied**.*

Options to configure the ESM to track successful events:

ACF2

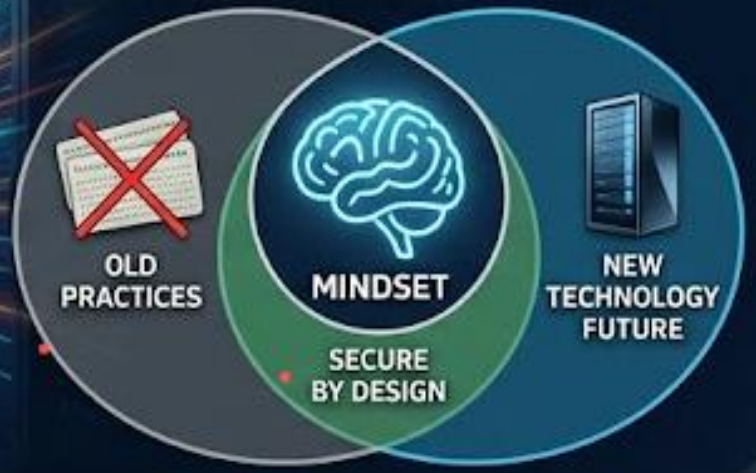
- **Sensitive Resources:** Use the LOG permission on individual access permissions within the rule (dataset or resource) or LOGPGM to log access to certain sensitive programs
- **Other Monitoring:** MONLOG cuts an audit record for system entry validation for a particular user. TRACE Specifies whether ACF2 creates SMF loggings for all data set and resource access attempts made by this user.

TSS

- **Sensitive Resources:** Apply the AUDIT attribute to specific ACIDs or Resources.
- *Command:* TSS ADD(dept) DSNAME(PAYROLL.) AUDIT
- **Global Options:** The LOG control option determines what gets written to the audit file. Setting LOG(ACCESS) or LOG(ALL) ensures that permitted accesses are captured alongside violations.

The Final legacy thing that needs to change....

The Last Legacy Component is YOU.



If system administrators do not pivot to **modern security principles...**

...everything we've discussed today about **zero-trust**, **logging**, and **governance** is just **theory**, not **protection**.

Move from ***permissive*** to ***principle of least privilege.***

Move from ***passive monitoring*** to ***proactive threat hunting.***

Move from ***reactionary fixes*** to ***automation and orchestration.***

SHARE
EDUCATE • NETWORK • INFLUENCE

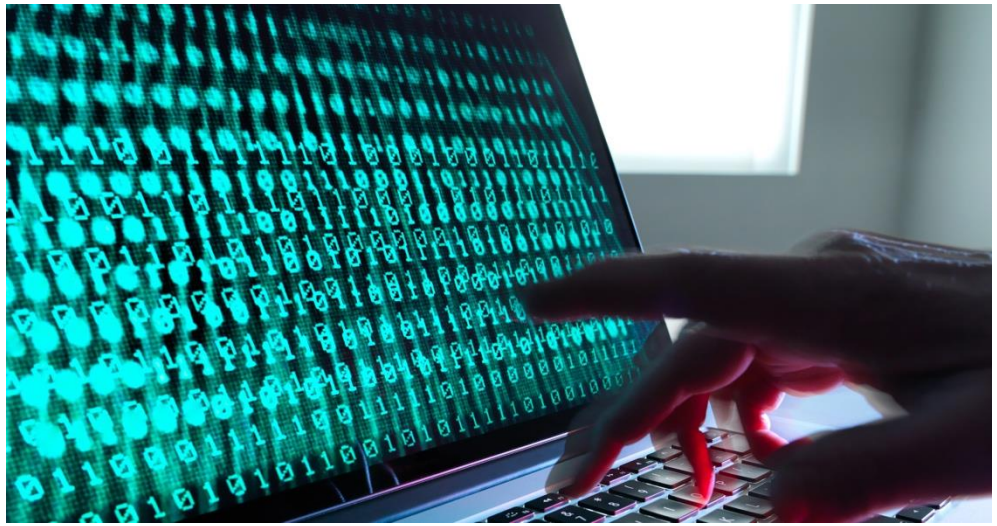
Thank You!

QR Code???

Hands-On Workshop: Ethical Mainframe Hacking (BYOD)

Join us for a **hands-on** opportunity to learn about ethical hacking and z/OS!

- Explore a vulnerable web application with a database backend,
- Learn the process of identification, fuzzing, iterating potential exploits
- Ultimately hacking into the mainframe's database



Location: **Room 409**

- Monday Aug 17 2:30-3:30pm
- Wednesday Aug 19 9:15-10:15am

Limited space — come early!

Upcoming Mainframe Conferences!

SHARE
EDUCATE • NETWORK • INFLUENCE

VSC 2026

Mainframe Technical Exchange™

Vanguard Security & Compliance

- Skillful instruction on cybersecurity threats, protection strategies, system configuration, and compliance in a proven format structured to provide the highest quality learning experience.
- Series of focused workshops and hands-on labs, attendees will have the opportunity to earn CPE credits.
- Sept 14-17, 2026 in Dallas TX

Broadcom Mainframe Technical Exchange

- Network with peers and Mainframe technical experts
- Participate in technical how-to sessions and hands-on workshops, hear product updates, provide feedback
- No registration fee! Virtual MTE
- Oct. 20-22, 2026 in North American MTE Plano, TX

GS UK | forge26

- The four-day in-person conference
- 'Forge' features keynote and plenary sessions, specialist technical streams, workshops, customer case studies, hands-on discussions, and community-led presentations covering a wide range of enterprise technology topics.
- Nov 2-5, 2026 in Whittlebury Park Towcester, UK

Technical Education Direct from the Experts

SHARE
EDUCATE • NETWORK • INFLUENCE

On-Demand Virtual

Virtual MTE
Access Sessions On-Demand through September 30, 2026

In-Person

North American MTE

Plano, TX
Oct. 20-22, 2026

Join a Mainframe Technical Exchange

- Network with peers and Mainframe technical experts
- Participate in technical how-to sessions and hands-on workshops, hear product updates, provide feedback
- No registration fee!

"The event covered all the relevant topics, and the content was amazing. The hands-on experience was also a good way to get actual experience with the tools."

Senthil Mathur, Manager, Accenture