#SHAREorg

SHARE
Technology · Connections · Results

Filling the Holes: Common Configuration Vulnerabilities in z/OS ACF2, RACF and Top Secret

Phil Emrich
Vanguard Integrity Professionals

Bill Valyo
CA Technologies

SHARE 120 – 3-8 February 2013
Session Number 12763

SHARE in San Francisco 2013

Who We Are

Bill Valyo

- Traditional IT Center:
  - Operator
  - Systems Programmer
  - Tech Support
  - IT Manager
- Consultant:
  - 18 Years and 4 Continents
  - Includes “Healthchecks” for ACF2, Etc.
- CA Technologies
  - Senior Consultant, North America

Phil Emrich

- Traditional IBM Technician for 31 Years
  - Dallas SysCntr – 22 Years
  - SMPO – 3 Years
- Consultant
  - 37 Years and 5 Continents
  - z/OS & RACF Security Assessments
  - RACF Migrations
- Vanguard Integrity Professionals, Inc.
  - Senior Consultant

About This Presentation

- We visit mainframe customers in a number of countries.
- We often see the same problems, repeatedly.
- We want to share these frequent problems and solutions.
- This is a combination of Phil and Bill’s “Top 10” lists.
  - Phil focuses on frequency and severity.
  - Bill focuses on severity only.
- We will try to get to all 10 (time-dependent)
- You do not need to know anything about these software tools at the start.
- The vulnerabilities are very much the same.

z/OS Exposure Severity Levels

- SEVERE (needs immediate remediation)
  - Immediate unauthorized access into a system
  - Elevated authorities or attributes
  - Cause system wide outages
  - The ability to violate IBM's Integrity Statement
- HIGH (needs remediation in the relatively near future)
  - Vulnerabilities that provide a high potential of disclosing sensitive or confidential data
  - Cause a major sub-system outage
  - Assignment of excessive access to resources.
- MEDIUM(needs a plan for remediation within a reasonable period)
  - Vulnerabilities that provide information and/or access that could potentially lead to compromise
  - The inability to produce necessary audit trails
- LOW (should be remediated when time and resources permit)
  - Implementation or configuration issues that have the possibility of degrading performance and/or security administration,

Bill's Training Approach:
General Compliance Principles

- Security by Default
  - Unless there is a specific permission to a resource, the user does not have permission to the resource.
- Individual Accountability
  - Each user of the system must be individually identifiable.
- Least Privilege
  - Each user should have only the access necessary to perform their job.

z/OS Access Control Systems

- z/OS Security, collectively called:
  - Access Control Systems (ACSs)
  - External Security Managers (ESMs)
- Tools:
  - ACF2
    - CA Technologies
  - RACF
    - IBM
  - Top Secret (TSS)
    - CA Technologies
- We are *not* promoting any individual tool...
  - …and are listing them alphabetically.

Configuration Components of ESMs:

Elements	ACF2	RACF	Top Secret
Option set is called:	GSO (Global System Opts.)	SETROPTS Options	Control Options
User ID is called:	LID (Logon ID)	User ID	ACID (Accessor ID)
Permissions are called:	Rules (linked by UID string)	Profiles & Access Lists	Permits
Permissions are found in:	Separate DBs for: • Datasets • Other Resources	RACF Database(s)	Kept in other ACIDs: • Profiles • Organizational • ALL Record

Excessive Number of IDs with Non-Expiring Passwords

- This is #1 on Phil’s “Top 10” list.
- Phil lists this as occurring in 67% of reviewed customers.
- Bill calls this an “Individual Accountability” compliance issue.
  - Passwords don’t expire, IDs are more likely to be stolen.
- We both agree that it is a SEVERE concern.

Excessive Number of IDs with Non-Expiring Passwords

- Value should be determined by your standards:
  - FISMA, PCI-DSS, HIPAA, NIST STIGs, etc.
  - Distributed environment
  - ITIL, ISO 27000 series, etc.
- Common values:
  - 30 days
  - 60 days (Phil: most common)
  - 90 days (Bill: most common)
- Use other controls to limit non-expiring passwords

Excessive Number of IDs with Non-Expiring Passwords

ACF2

- Set in GSO PSWD record
  - PSWDMAX keyword.
- May be overridden in LID
  - LIST LIDS > x days
- Non-expiring privileges:
  - RESTRICT - no password required.
  - PGM(program) – must be submitted from this program
  - SUBAUTH – must come from APF.

RACF

- SETROPTS command
  - PASSWORD(INTERVAL(..)) keyword
- User profile my only specify a shorter interval or NOINTERVAL
- Non-expiring privileges:
  - PROTECTED – no password.

Top Secret

- PWEXP Control Option
  - Only for new users
  - See also INACTIVE option.
- Overridden by:
  - HPBPW – Honor expired batch password specified number of additional days.
- Non-expiring recommendations:
  - Don't use NOSUBCHK attribute.
  - Use ACID and PRIVPGM together.

Inappropriate Use of USS Superuser

- This is #2 on Phil's "Top 10" list.
- Phil lists this as occurring in 55% of reviewed customers.
- Bill calls this a "Security by Default" compliance issue.
  - Superusers are virtually unlimited.
- We both agree that it is a SEVERE concern.

Inappropriate Use of USS Superuser

- These are user IDs with the UID set to 0 (zero)
- No user IDs for people need UID(0).
- Should be limited to USER IDs for UNIX deamons.
- Servers generally should *not* have UID(0).
  - Use resource rules like FACILITY.BPX.SERVER, etc.
  - Call vendor if their manual says to use UID(0).

Inappropriate Use of USS Superuser

ACF2

- UID(0) is not to be confused with ACF2 UID string.
- Set in LID.

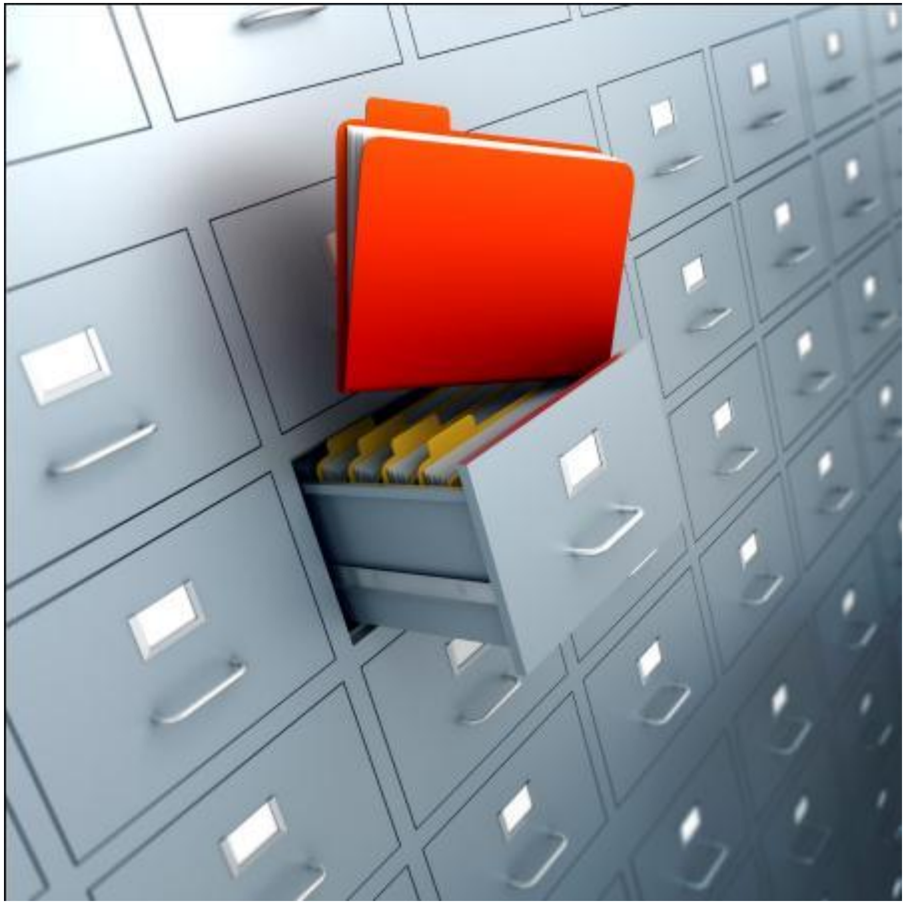
RACF

- UID(0)
- Set in OMVS Segment of User profile

Top Secret

- Assigned in the ACID by the UID keyword.
- Related config:
  - OPTIONS control option number 74 determines if non-SCA can administer these.

Excessive Number of Data Sets with Universal Access Greater than READ



- This is #3 on Phil's "Top 10" list.
- Phil lists this as occurring in 54% of reviewed customers.
- Bill calls this a "Least Privilege" or "Security by Default" compliance issue.
  - You are overriding controls for a large set of users.
- We both agree that it is a SEVERE concern.
- Relates to how the site defines access (above READ).

Excessive Number of Data Sets with Universal Access Greater than READ

ACF2

- Ruleset entries with:
  - UID(*)
- And:
  - WRITE(A)
  - UPDATE(A)
- DECOMP rules to sequential file and do ISPF “FIND” on UID(*) string.

RACF

- Profiles with:
  - UACC(UPDATE) or ALTER
  - Or an ID(*) access list entry with ACESS(UPDATE) or ALTER

Top Secret

- ALL Record
  - In effect, an ACID that all users are defined to.
  - ACCESS keyord levels:
    - CREATE
    - DELETE
    - PURGE
    - REPLACE
    - SCRATCH
    - UPDATE
    - WRITE
    - Etc.
- Use
  - TSS LIST(ALL)

Excessive Access to APF Libraries

- This is #4 on Phil’s “Top 10” list.
- Phil lists this as occurring in 40% of reviewed customers.
- Bill calls this a “Least Privilege” compliance issue.
  - Most users should not have APF access.
- We both agree that it is a SEVERE concern.

Excessive Access to APF Libraries

ACF2

- APF libraries protected only by specific rule keys:
  - e.g. $KEY(SYS1)
- Should be no universal access
  - e.g. UID(*)…

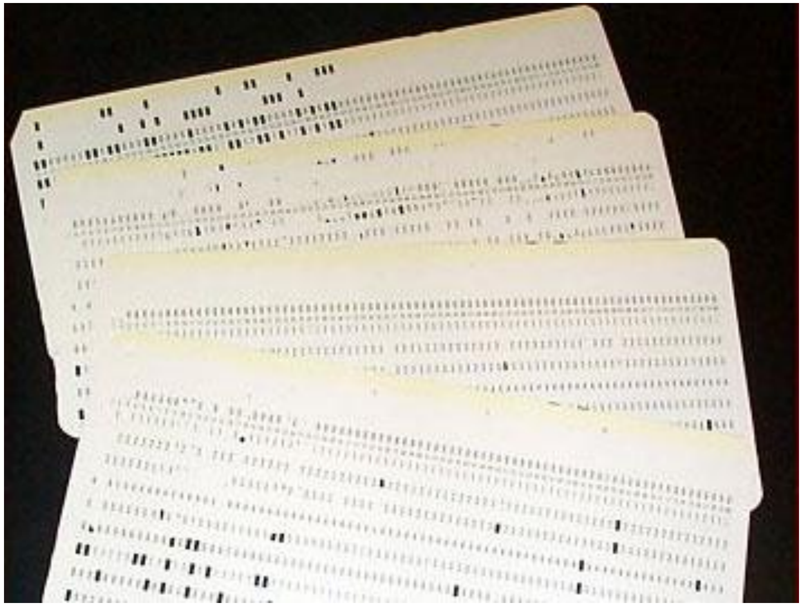
RACF

- APF libraries protected only by very generic profiles:
  - e.g. SYS1.*.**
- APF libraries should be protected by a fully qualified generic profile:
  - SYS1.LE.SCEERUN
- Acceptable exceptions:
  - SYS2.CA7.
    R%%%.CAL2LOAD

Top Secret

- PERMIT function to specific libraries.
- Good idea to create separate PROFILE for APF libraries.

Production Batch Jobs with Excessive Data Set or Resource Access



- This is #5 on Phil's "Top 10" list.
- Phil lists this as occurring in 39% of reviewed customers.
- Bill calls this a "Security by Default" compliance issue.
  - Highly privileged batch IDs can access virtually anything.
- We both agree that it is a SEVERE concern.

Production Batch Jobs with Excessive Resource Access

ACF2

- Recommend separate LIDs by application (at least).
- Recommend no bypassing privileges, such as:
    - NON-CNCL
    - SECURITY without RSCVLD and RULEVLD
    - Potentially others.

RACF

- Batch User IDs with the OPERATIONS attribute
- OPERATIONS allows ALTER access to all Data Sets unless specifically denied in the covering profile
- OPERATIONS does not allow access to general resources unless explicitly specified in the class definition.

Top Secret

- Recommend separate ACIDs by application (at least).
- Recommend no bypassing privileges, such as:
    - BYPASS
    - NORESCHK
    - NODSNCHK
    - Potentially others.

Use of Warn (or Other) Modes

- This is #6 on Phil's "Top 10" list (sort of).
  - Phil lists: General Resource Profiles in WARN Mode
  - Bill has found: Other modes and not always limited to specific resources
- Phil lists this as occurring in 37% of reviewed customers.
- Bill calls this *the* "Security by Default" compliance issue.
- We both agree that it is a SEVERE concern.

Use of Warn (or Other) Modes

- All ESMs have a MODE definition.
- Determines *if* and *where* security is turned on.
- Used for:
  - Initial migration to ESM security (decades ago)
  - Migration to security for new applications (sometimes)
- Often:
  - Forgotten
  - Abused

Use of Warn (or Other) Modes

ACF2

- RULEOPTS GSO:
  - MODE keyword.
- Values:
  - ABORT (security on!)
  - WARN (send msg only)
  - LOG (log only)
  - IGNORE (do nothing)
  - RULE (override at rule)
- May be overridden in the rule:
  - This is typically a problem as the RULE option is not understood.
- Is for dataset rules only.

RACF

- SETROPTS
  - NOPROTECTALL
  - PROTECTALL
- Values:
  - WARNING
  - FAILURES
- Requires a profile covering a data set to allow any access
- Applies only to data sets

Top Secret

- MODE Control Option
- Values:
  - FAIL (security on!)
  - WARN (send msg only)
  - IMPL (doesn't include undefined users and resources)
  - DORMANT (do nothing)
- May be overridden by:
  - ACTION on a permission
  - Facility
  - Specific user permission
  - DRC (detailed reason code) control option

Started Task IDs not Properly Protected

- This is #7 on Phil’s “Top 10” list.
- Phil lists this as occurring in 46% of reviewed customers.
- Bill calls this a “Security by Default” compliance issue.
  - STCs should not be immune to security controls.
- We both agree that it is a HIGH concern.

Started Task IDs not Properly Protected

ACF2

- OPTS GSO record:
  - STC keyword
- Define LIDS for each STC.
  - By START command USER keyword
  - Through optional GSO STC table
  - By name of STC procedure (most common)
  - Do not use DFTSTC unless it is a “dummy” LID.
- Define “STC” privilege in each STC LID.

RACF

- User IDs for Started Tasks should be PROTECTED (i.e. no password)
- Prevents revocation for sign-on attempts or User ID inactivity
- Prevents misuse if password were to become known

Top Secret

- Implement an STC Facility
- Define LIDS for each STC (*TSS manuals do not require, but I do*).
  - Use STC Table by PROCNAME.
  - Recommend NOPW ACIDs.
- ACID must be granted access to STC Facility.

Excessive Number of Data Sets with Universal READ Access

- This is #8 on Phil's "Top 10" list.
- Phil lists this as occurring in 42% of reviewed customers.
- Bill calls this a "Least Privilege" or "Security by Default" compliance issue.
  - You are overriding controls for a large set of users.
- We both agree that it is a HIGH concern

Excessive Number of Data Sets with Universal READ Access

ACF2

- Ruleset entries with
  - UID(*)
- And…
  - READ(A)

RACF

- Profiles with:
  - UACC(READ)
  - Or an ID(*) access list entry with ACESS(READ)

Top Secret

- ALL Record
  - In effect, an ACID that all users are defined to.
  - ACCESS keyword level:
    - READ
- Use
  - TSS LIST(ALL)

Excessive Number of IDs with Privileged Attributes

- This is #9 on Phil’s “Top 10” list.
- Phil lists this as occurring in 38% of reviewed customers.
- Bill calls this a “Least Privilege” compliance issue.
  - You are overriding permissions, often providing access to all resources.
- We both agree that it is a HIGH concern.

Excessive Number of IDs with Privileged Attributes

ACF2

- Avoid or severely limit use of:
  - NON-CNCL
  - READALL
  - SECURITY (without RULEVLD and RSCVLD)
  - Others
- Create means for emergency ID access as alternative.
- Document conditions where necessary.

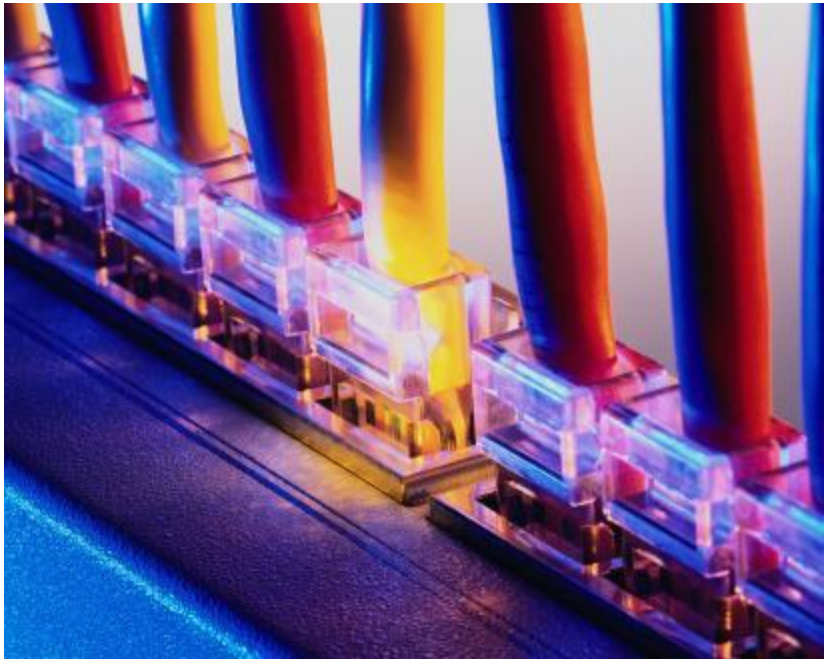
RACF

- SPECIAL, OPERATIONS and AUDITOR attributes should be assigned to the smallest number of individuals that is practical.

Top Secret

- Avoid or severely limit use of:
  - BYPASS
  - NODSNCHK
  - NORESCHK
  - Others
- Create means for emergency ID access as alternative.
- Document conditions where necessary.

Improper Use or Lack of Control for UNIX System Services



- This is #10 on Phil's "Top 10" list.
- Phil lists this as occurring in 37% of reviewed customers.
- Bill calls this a "Least Privilege" compliance issue.
  - Use BPX as alternative to "root"
  - Limit use of traditional UNIX security commands
- We both agree that it is a HIGH concern.

Improper Use or Lack of Control for UNIX System Services

ACF2

- FACILITY class
  - BPX.xxxxx Profiles
    - BPX.DAEMON
    - BPX.FILEATTR.*
    - BPX.SERVER
    - BPX.SUPERUSER
    - etc.
- UNIXPRIX class
  - CHOWN.UNRESTRICTED
  - SUPERUSER.FILESYS
  - SUPERUSER.
    FILESYS.CHOWN
  - etc.

RACF

- FACILITY class
  - BPX.xxxxx Profiles
    - BPX.DAEMON
    - BPX.FILEATTR.*
    - BPX.SERVER
    - BPX.SUPERUSER
    - etc.
- UNIXPRIX class
  - CHOWN.UNRESTRICTED
  - SUPERUSER.FILESYS
  - SUPERUSER.
    FILESYS.CHOWN
  - etc.

Top Secret

- FACILITY class
  - BPX.xxxxx Profiles
    - BPX.DAEMON
    - BPX.FILEATTR.*
    - BPX.SERVER
    - BPX.SUPERUSER
    - etc.
- UNIXPRIX class
  - CHOWN.UNRESTRICTED
  - SUPERUSER.FILESYS
  - SUPERUSER.
    FILESYS.CHOWN
  - etc.

Thanks! (Session # 12763)

Phil Emrich	Bill Valyo
Phil.Emrich@Go2Vanguard.com	William.Valyo@CA.com

See you in Boston in August!