(E)JES® Security

April 20, 2016

Presented by Ed Jaffe
edjaffe@phoenixsoftware.com

PHOENIX Software International®
SOLUTIONS FOR MAINFRAME AND PC PLATFORMS

Sources of Security Decisions

- Internal Security
  - Always checked first, even when SAF security in effect
  - **Note:** This is an important differentiator with SDSF
- SAF Security
  - Checked only if action allowed by internal security
  - In general, we recommend customers use SAF security augmented by internal security where necessary.
- User Exits
  - Minimal but important decision-making capabilities

Internal Security

Internal Security

- Macro-based Specifications
  - EJESUM2 macro provides security for JES2 customers
  - EJESUM3 macro provides security for JES3 customers
  - Security specifications saved in EJESPRM2 and EJESPRM3 load modules located in SEJELINK.
- Parametrized Specifications
  - Parmlib member (IEFPRMLB service used)
  - EJESPSEC TSO/E command used to check/activate
  - Resulting security policy stored in CSA

Macro-based Internal Security Specifications

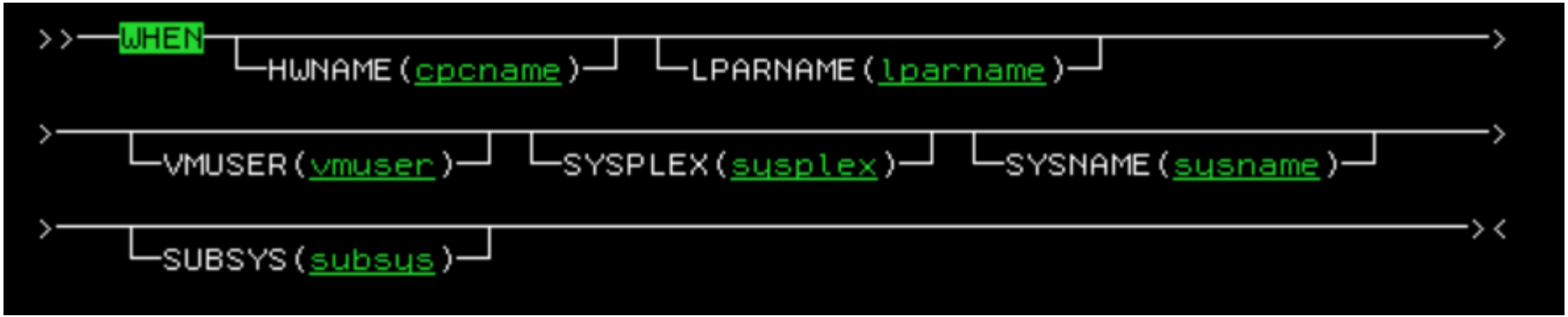
- EJESUM2 macro is used for JES2 environments
- EJESUM3 macro is used for JES3 environments
- The source member is assembled and linked to produce the EJESPRM2 or EJESPRM3 load module.
  - Normally installed via SMP/E USERMOD EJESPRM
  - Each module represents a single security policy
- The load module appropriate to the JES being accessed is fetched by an MVS LOAD SVC issued during (E)JES session initialization.

Parametrized Internal Security Specifications

- Can reside in system parmlib concatenation
  - IEFPRMLB service used to read member contents
- Can describe multiple environments
  - Statements to be processed are identified by an optional WHEN statement(s) envelope
- EJESPSEC TSO/E command used to activate policy
- Current and previous policies are stored in ECSA and located by system-level Name/Token
- Back-out possible using EJESPSEC SWITCH

Security Policy Environment Selection

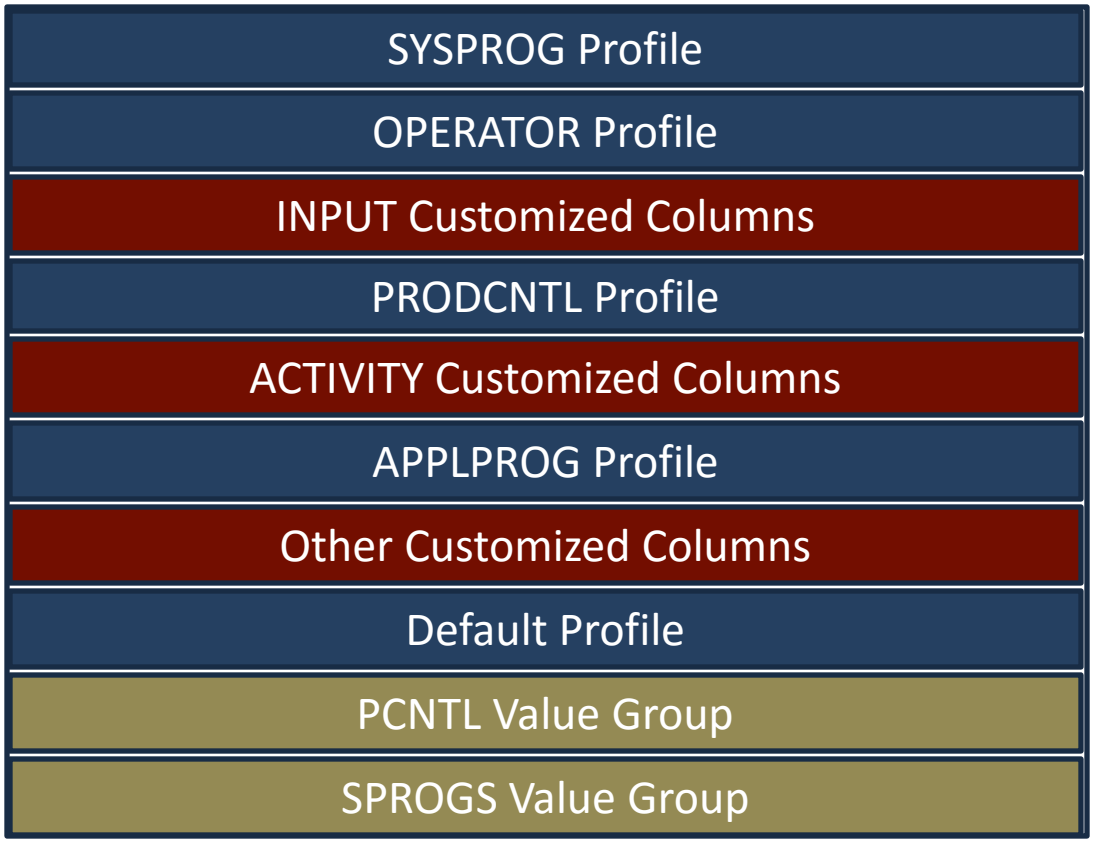
- All specified environmental attributes are checked. If any do not match, all records are skipped until the next WHEN statement is encountered.
- Wildcard matching is not performed. All values must be an exact match.



Security Policy Contents

- A security policy contains security profiles and (optionally) value groups and customized column lists.
- The order in which the profiles and column lists appear is important since matching is performed in a top-down manner.
  - Value groups can appear anywhere.
- A default profile is one with no matching keywords. If multiple such profiles are discovered, the last one is used.

Sample Security Policy Specifications



- Five security profiles, three customized column lists, and two value groups.

Security Profile Matching

- Profile matching occurs in a top-down manner and may be done using session attributes, TSO/E authorizations, or SAF checking READ access to EJESPROF.profname (this is recommended).
- When a profile is matched, the most recent customized column list for any given display is used.
- If no profile is matched, the last default profile is used. If no default profile exists, access is denied.

Security Profile Matching

- Session attributes matching:
  - Single or value group mask matching against userid, SXID (value provided by user exit – usually the current SAF group name from the ACEE), terminal name, and/or JCL procedure name.
- TSO/E authorizations matching:
  - TSO/E OPER, ACCT, MOUNT, or JCL
  - In non-TSO environments, these attributes are tested by SAF checking against resources in the TSOAUTH class. (UADS is never accessed by (E)JES.)

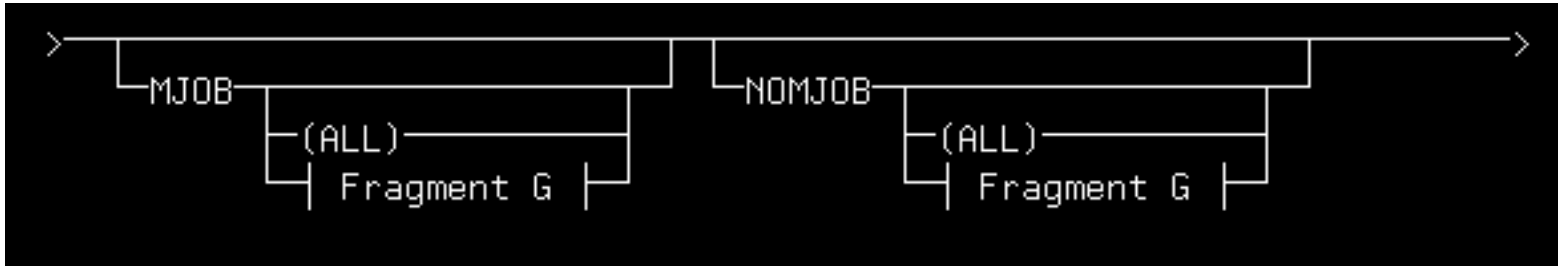
Security Profile Components

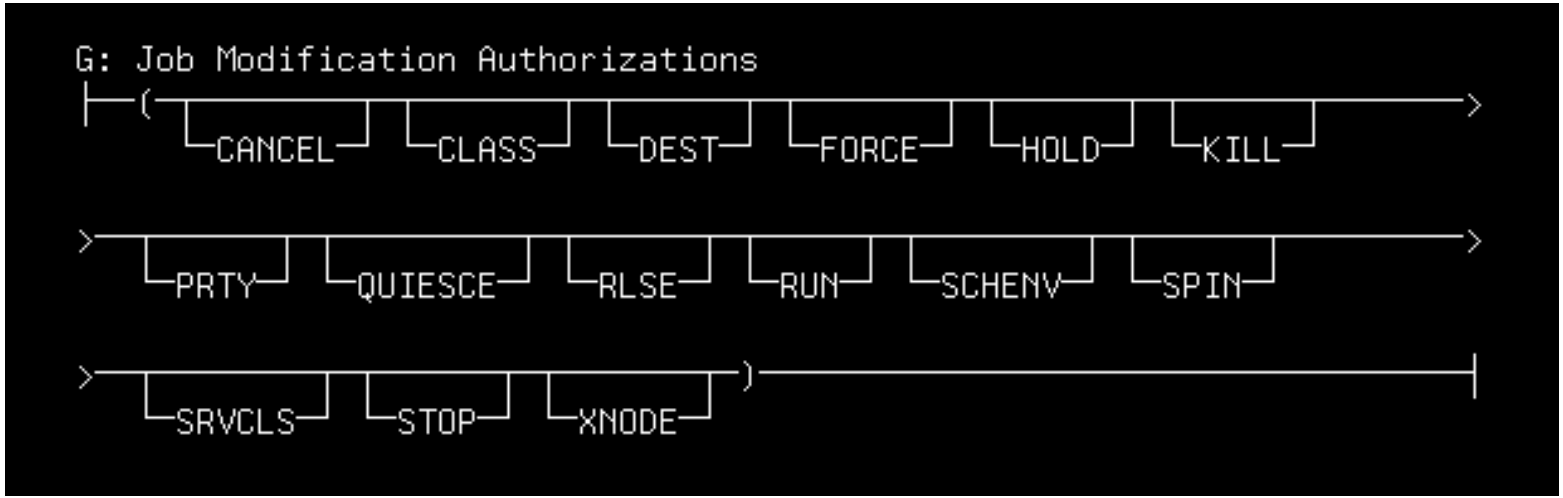
- Function Authorizations
  - Controls authority to use various (E)JES functions e.g., to invoke the Activity display or hold/release jobs.
- User Settings
  - Not used to protect system resources. They specify miscellaneous things such as the default code page, command logging options, etc.
- View and Alter Include/Exclude Lists
  - Controls access to jobs and output based on matching of attributes such as owning userid, job name, job class, sysout class, destination, etc.

Function Authorizations

- Some function authorizations are stand-alone specifications, such as [NO]TRACE or [NO]ABEND.
- Others, such as [NO]MJOB, are implemented as an include/exclude list (parametrized) or as a two-tier hierarchy (macro keywords).
- MJOB(ALL) or MJOB=YES
  - Allow all job modifications
- NOMJOB(ALL) or MJOB=NO
  - Disallow all job modifications

Function Authorizations





Function Authorizations

- Either specify the functions you want:
  - MJOB(CANCEL HOLD RLSE DEST CLASS PRTY)
  - Allow cancel, hold, release and overtype of destination, job class, and priority.
- Or specify the functions you don’t want:
  - NOMJOB(FORCE)
  - Allow all job modifications except force

View and Alter Include/Exclude Lists

- VAIELs control which jobs or output can be viewed and/or altered. A user can always view and alter his/her own jobs. Therefore, VAIELs apply only to jobs owned by others.
- Comparison masks can be a single value or a list of values and may include references to one or more value groups (a way of sharing a list of values across multiple specifications).

View and Alter Include/Exclude Lists

- The outcomes of comparing multiple values against a single attribute are Boolean ORed.
- By default, the outcomes of comparisons involving different attributes are Boolean ANDed. However, you can request Boolean ORing for include processing with VIBOOL(OR) and/or AIBOOL(OR).

View and Alter Include/Exclude Lists

- VIOWNR(SYSOPER PRODCNTL SUP*)
  - Allow viewing if the job is owned by SYSOPER or by PRODCNTL or by userids that start with SUP
  - The view action includes display on a tabular panel, therefore jobs not viewed also cannot be altered.
- AXOWNR(SYSOPER PRODCNTL SUP*)
  - Disallow alteration if the job is owned by SYSOPER or by PRODCNTL or by userids that start with SUP.

View and Alter Include/Exclude Lists

- VIOWNR(SYSOPER PRODCNTL SUP*) VIJNAM(PROD* TEST*)
  - Allow viewing if the job is owned by SYSOPER or by PRODCNTL or by userids that start with SUP
  - **AND**… if the jobname starts with PROD or with TEST
- VIOWNR(SYSOPER PRODCNTL SUP*) VIJNAM(PROD* TEST*) VIBOOL(OR)
  - Allow viewing if the job is owned by SYSOPER or by PRODCNTL or by userids that start with SUP
  - **OR**… if the jobname starts with PROD or with TEST

Global Profiles

- Global profiles are defined using syntax similar to what's used to define a normal security profile, but they don't take up space in the security policy.
- Rather, they provide default function authorizations and user settings to be used for security profiles subsequently defined in the input stream.
- Every global profile definition completely replaces any previous global profile. They are not additive.
- This can greatly minimize the amount of textual specification needed to generate a policy.

Global Profile Example

- **TRACE** is the default if not specified.
  - Typical. Virtually everything defaults to enabled.
- To disallow TRACE for the majority of security profiles without using global profiles, you must explicitly specify **NOTRACE** as appropriate.

```
PROFILE NAME(name1)                 … (other specifications)
PROFILE NAME(name2) NOTRACE         … (other specifications)
PROFILE NAME(name3) NOTRACE         … (other specifications)
PROFILE NAME(name4) NOTRACE         … (other specifications)
PROFILE NAME(name5) NOTRACE         … (other specifications)
PROFILE NAME(name6) NOTRACE         … (other specifications)
PROFILE NAME(name7)                 … (other specifications)
PROFILE NAME(name8) NOTRACE         … (other specifications)
```

Global Profile Example

- In this example, a GBLPROF is defined to make **NOTRACE** the default for all subsequent profiles.

```
GBLPROF                    NOTRACE     … (other specifications)
PROFILE NAME(name1)        TRACE       … (other specifications)
PROFILE NAME(name2)                    … (other specifications)
PROFILE NAME(name3)                    … (other specifications)
PROFILE NAME(name4)                    … (other specifications)
PROFILE NAME(name5)                    … (other specifications)
PROFILE NAME(name6)                    … (other specifications)
PROFILE NAME(name7)        TRACE       … (other specifications)
PROFILE NAME(name8)                    … (other specifications)
```

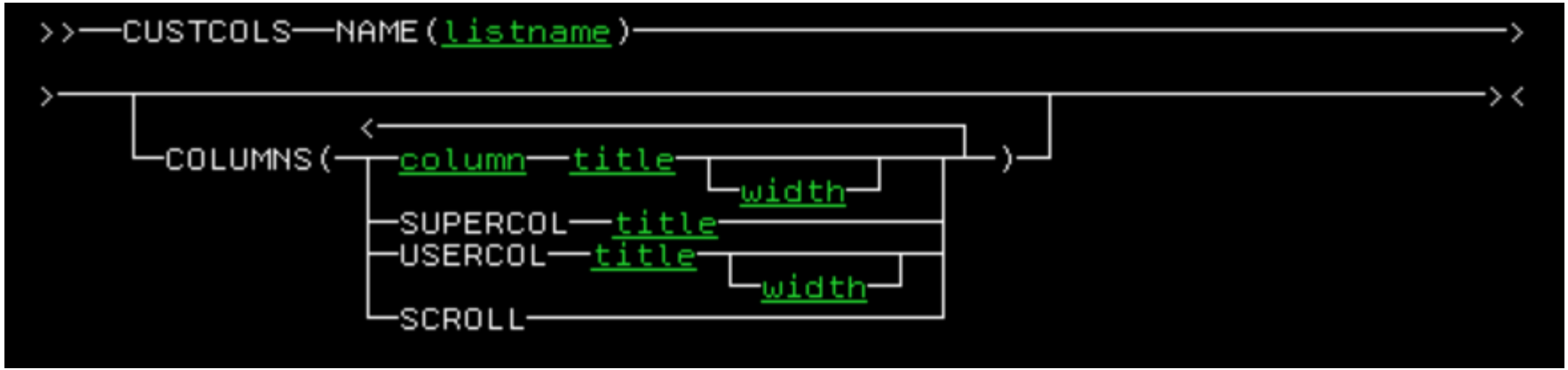
Value Groups

- VGROUP NAME(ABC) VALUES(FRED* PAUL*)
  - Creates a reusable list of the masks FRED* and PAUL*
  - VIOWNR(FRED* PAUL*) ➔ VIOWNR(G=ABC)
- You can specify a value group reference as just one term in a larger list:
  - VIOWNR(SYSOPER PRODCNTL G=ABC SUP*)
  - VIOWNR(SYSOPER G=ABC PRODCNTL G=DEF SUP*)

Customized Column Lists

- Only the installation can change column titles and permanently hide columns from users.
- Nevertheless, we don’t recommend customized column lists for various reasons, including:
  - Users can rearrange or hide columns and the scroll point. They can change column widths as needed.
  - Creating and maintaining the lists is tedious and complex
  - Over time the lists become obsolete, but updating them with the latest columns is ~~almost~~ never done.

Customized Column Lists



- A “super” column is a title that spans across more than one column. For example, the title **Translate-Tables** spans across the **CHAR1**, **CHAR2**, **CHAR3** and **CHAR4** columns.

External (SAF) Security

External (SAF) Security

- Uses resources defined in the EJES and optionally JESSPOOL, WRITER, OPERCMDS, and XFACILIT resource classes
  - Recommend use SDSF instead of EJES to avoid CDT
- SAF consulted only for actions allowed by internal security checking
  - A SAF-only implementation works with the default internal security specifications delivered with (E)JES because everything is allowed by default.
  - Internal security can be added as needed to supplement

Activating SAF Security

- Specify security package name on SAFTYPE:
  - SAFTYPE(RACF|ACF2|TOPS)
- Specify classes to be used. Use blank or null placeholder for an unused class or an asterisk to use the default name:
  - SAFRCLS(SDSF * * * * *)
  - Asterisk placeholders imply EJES, JESSPOOL, WRITER, OPERCMDS, JESSPOOL, and XFACILIT class names
  - First JESSPOOL entry for jobs; second for data sets. (This was needed decades ago to cope with restrictions in generic mask naming syntax in Top Secret. Unknown if this is still an issue.)
- Ensure the EJES (or this case SDSF) class is active
- Define EJESAUTH.ENTRY resource with UACC(READ)

SAF Resource Classes

Class	Resource	Description
EJES (or SDSF)	EJESCMD (hlq) EJESATTR (hlq) EJESVAL and EJESCHG (hlq) EJESAUTH (hlq) EJESPROF (hlq) EJESOPER (hlq) EJESelmt.element.identification	Primary commands Line commands and overtypes Existing and new overtype values Specific authorizations Internal security profiles System commands and DOA Access to unarchitected elements
WRITER	jesx.type.devicename	Printers and Punches
JESSPOOL	node.owner.jobname.jobid node.owner.jobname.jobid.Ddsnum.dsname	Altering jobs and groups Browsing spool data sets
OPERCMDS	MVS (hlq) or JES2 (hlq) or JES3 (hlq)	EMCS consoles and commands
XFACILIT	HZS.sysname.owner.checkname.action	Health checker resources

SAF Resource Characteristics - Names

- SAF resource names are designed to facilitate the use of generics to minimize the number of resource profiles needed.
- Attribute.DisplayType.DisplayName.Column
  - EJESATTR.OUTPUT.HOLD.FORM
  - EJESATTR.OUTPUT.OUTPUT.FORM

SAF Resource Characteristics - Levels

- Access levels are designed to group functions of similar “destructiveness” together at each level: READ, UPDATE, CONTROL and ALTER.
  - EJESATTR.JOB.CANCEL UPDATE
  - EJESATTR.JOB.CLASS CONTROL
  - EJESATTR.JOB.FORCE ALTER
    - Most job attributes require UPDATE
    - Job scheduling attributes require CONTROL
    - More potentially-destructive functions require ALTER

Unconditional JESSPOOL Access

- SAF checking of resources in the JESSPOOL class is skipped for the job owner in a manner similar to what's done for Internal Security View and Alter Include/Exclude Lists.
- This unconditional access is also extended to the job submitter via the SUBUACC installation option.

Destination Operator Authority

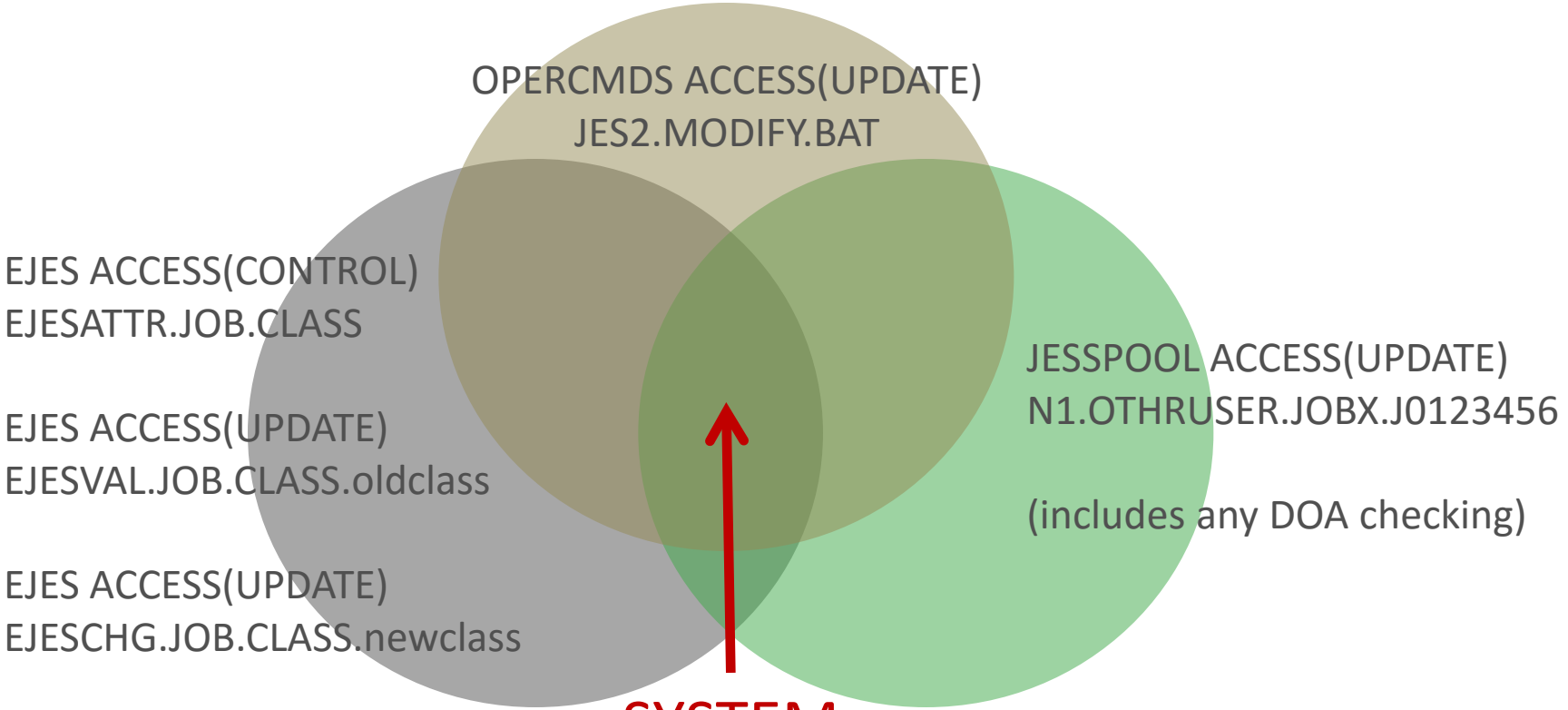
- Provides pre-JESSPOOL SAF checking for operators and others with a need for system wide authorities.
- The most common configuration is shown in this table.

Resource Name	UACC	Operator Access
EJESOPER.DEST.**	NONE	READ
EJESAUTH.DEST.*	ALTER	-
EJESAUTH.DEST.*.DATASET.JESMSGLG	READ	-
EJESAUTH.DEST.*.DATASET.JESJCL	READ	-
EJESAUTH.DEST.*.DATASET.JESYSMSG	READ	-

Protecting Overtypes

- EJESATTR protects the column from overtype
  - EJESATTR.JOB.CLASS
- EJESVAL protects existing values in the column
  - EJESVAL.JOB.CLASS.xxxxxxxx
- EJESCHG protects new values in the column
  - EJESCHG.JOB.CLASS.xxxxxxxx
- Sample Use Case: You could prevent users from submitting with class FASTBAT, but allow them to perform an ad-hoc change from SLOWBAT to FASTBAT while protecting all other class names.

SAF Checking Overlap



Sample SAF TRACE

```
EJES511 EDJX2    SDSF     - D A 00 SAF EJESAUTH.SUBUACC.PHXHQ
EJES511 EDJX2    SDSF     - D R 00 SAF EJESOPER.DEST.PHXHQ
EJES511 EDJX2    SDSF     - D R 04 SAF EJESCMD.USERDISP.STATUS.PHXHQ
EJES511 EDJX2    SDSF     - D C 00 SAF EJESATTR.JOB.PRTY
EJES511 EDJX2    SDSF     - D C 04 SAF EJESATTR.JOB.CLASS
EJES511 EDJX2    SDSF     - D C 04 SAF EJESATTR.JOB.SRVCLASS
EJES511 EDJX2    SDSF     - D U 00 SAF EJESAUTH.DEST.LOCAL
EJES511 EDJX2    JESSPOOL L M U 00 SAF PHXHQ.RMULLIN.RMWTOR.J0197129
EJES511 EDJX2    SDSF     L D U 04 SAF EJESVAL.JOB.CLASS.A
EJES511 EDJX2    SDSF     L D U 04 SAF EJESCHG.JOB.CLASS.B
EJES511 EDJX2    OPERCMDS L D U 00 SAF JES2.MODIFY.BAT
EJES511 EDJX2    OPERCMDS L D R 00 SAF MVS.MCSOPER.EDJX2
IEA630I  OPERATOR EDJX2    NOW ACTIVE,   SYSTEM=MVSA0    , LU=ISZ004
EJES510 USER-EDJX2--- $TJ(197129),C=B
$TJ(197129),C=B
$HASP890 JOB(RMWTOR) 721
$HASP890 JOB(RMWTOR)    STATUS=(AWAITING HARDCOPY),CLASS=B,
$HASP890                PRIORITY=1,SYSAFF=(ANY),HOLD=(NONE)
```

Security-Related User Exits

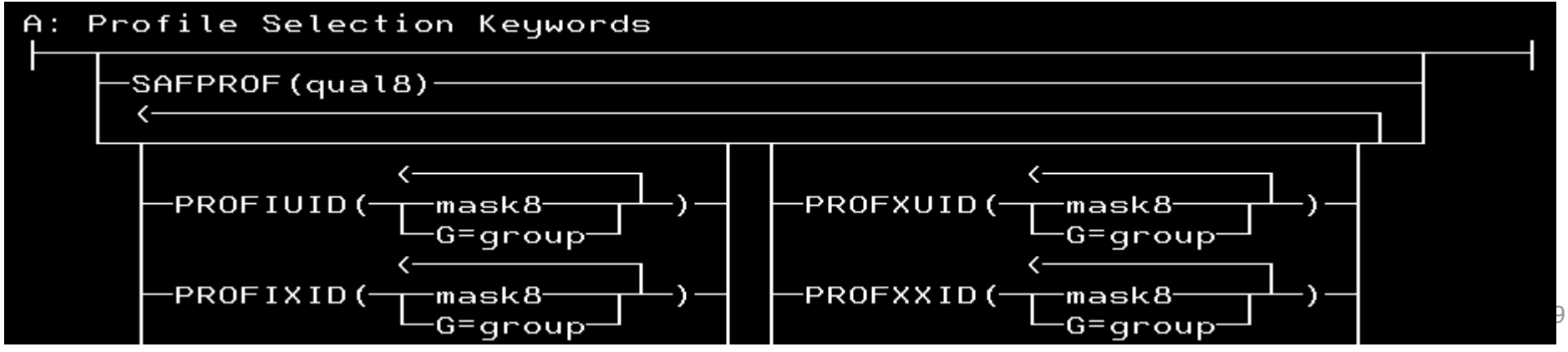
Security-Related User Exits

- The following user exits provide direct support of security-related decisions and can be used in a variety of useful ways.

Exit Name	Function	Comments
EJESUX01	Userid to SXID translation	
EJESUX05	Provide MVS/JES Cmd Auth Level	Used with Internal Security only
EJESUX06	SAF Command Resource Modification	
EJESUX07	SAF Services	
EJESUX09	Extended Submitter Validation	
EJESUX14	User Security Extensions	Needed for ISFPARMS XDSP()

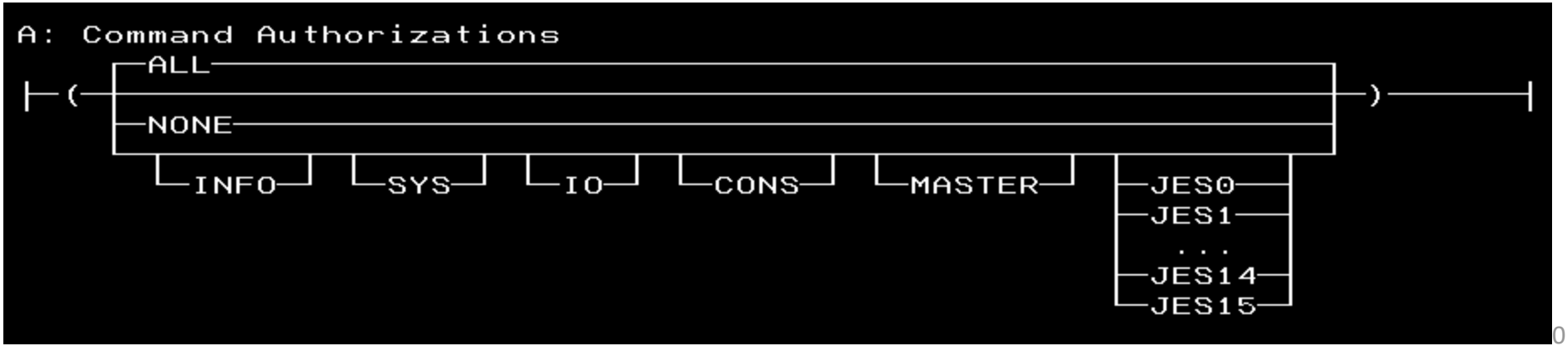
EJESUX01 - Userid to SXID Translation

- Not very popular after list of groups checking
- Purpose: Populate the SXID given userid as input
- Internal Security allows SXID to be used in a manner similar to userid for profile selection, View and Alter Include/Exclude checking, etc.



EJESUX05 - Provide MVS/JES Cmd Auth Level

- Internal Security CMDS keyword supports old-style MVS console authority keywords and a JES level
- EJESUX05 parses the command string and returns one of these attributes to the command driver.



EJESUX06 - SAF Cmd Resource Modification

- Special exit point just for OPERCMDS resources
- Input: original command and SAF resource
- Resource name can be modified or left alone
- Intended as a migration aid for customers with "home grown" SAF command security
- Return codes:
  - 00 – continue with SAF call
  - 04 – unconditionally accept the command
  - 08 – unconditionally reject the command

EJESUX07 - SAF Services

- All SAF calls go through this exit
  - Extract TOKEN (TOKENXTR)
  - MAP Token to internal or external form (TOKENMAP)
  - Perform authorization check (AUTH)
  - Create and delete security environment (VERIFY)
- Entity name can be changed as a migration aid for customers with “home grown” SAF security needs
- Return code must be SAF return code: 0, 4, or 8

EJESUX09 - Extended Submitter Validation

- Remember SUBUACC? It can be extended to users other than the actual submitting user
- Controlled by [NO]SUBXTND in Installation Options
- Input: owning userid, submitting userid, jobname, and notify userid (if available)
- Return codes:
  - Zero – Current user treated like submitter
  - ¬Zero – Current user *not* treated like submitter

EJESUX14 - User Security Extensions

- Provides additional security decision points
- The only supported call right now is "**Data Set Browse Authority**" (ESXRBROW)
- Data passed includes:
  - Job name, job ID, job type, job number, job owner
  - Proc name, step name, DD name, DSNUM, DSNAME
  - Sysout class, System ID (if executing), Origin/Destination, External writer name, SAF Security token

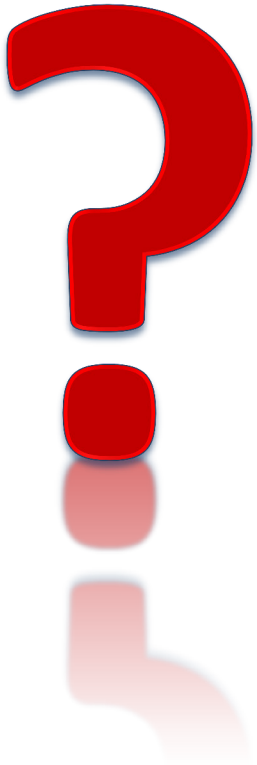
EJESUX14 - User Security Extensions

- Return codes:
  - 00 – Continue normal authorization
  - 04 – Unconditionally accept the action
  - 08 – Unconditionally reject the action
- Needed to provide 100% equivalency to XDSP in ISFPARMS since (E)JES View exclusion prevents appearance on tabular display
- ISFPARMS XDSP applies only to the browse action
- We have a design draft to add Internal Security Browse Include/Exclude, but that does not exist yet

Questions?

Contact Information:

Phoenix Software International
831 Parkview Drive North
El Segundo, CA 90245
http://www.phoenixsoftware.com
sales@phoenixsoftware.com



PHOENIX Software International®