Hayim Sokolsky
ae35.net

# Batch Security: Life of a Job



The adventures, trials, and tribulations of your average batch job in the big land of ~~MVS~~, ~~MVS/SP~~, ~~MVS/XA~~, ~~MVS/ESA~~, ~~OS/390~~, z/OS, [insert next name here].

## Or just....
## "Life of a Job"

## About the presenter

- Hayim Sokolsky has been a Security Architect, Systems Programmer, _____ (job title), _____ (another job title), etc..., for over __ (number) years, with __ (number) years of RACF and security related experience.
  He _____ (verb) _____ (noun) in establishing and customizing controls for RACF, z/OS, JES_ (number), ICSF, SDSF, DB2, _____ (product name) and other systems software.

 Real World RACF/DB2 3

"the dark ages"

## Batch History

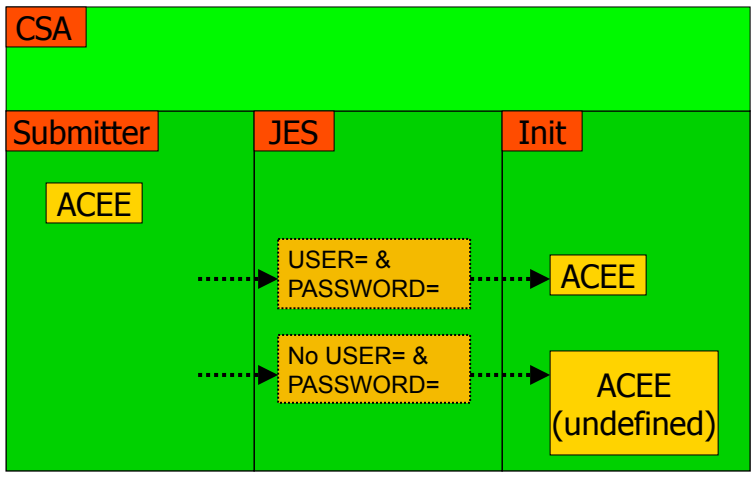
4  Life of a Job

# Cro-Magnon Job (MVS, MVS/SP)

- In the early dawn of MVS, before MVS/XA, the "Life of a Job" was simple
  - Job submitted without USER= on the job card executed with no assigned UserID, a.k.a. "undefined"
  - Job submitted with a valid USER= and PASSWORD= ran with the authority of the UserID

 Life of a Job 5

# Cro-Magnon Job



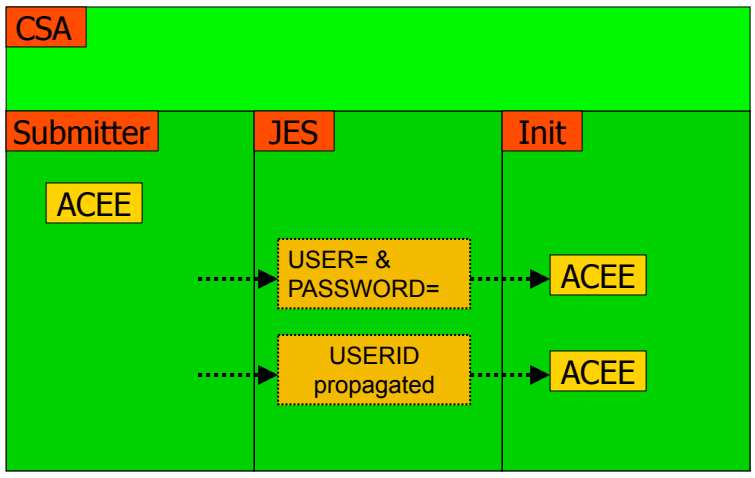

 Life of a Job 6

# The Renaissance Job (MVS/XA)

- Starting with MVS/XA 2.2 (MVS/SP 2.2.0)
  - Locally submitted jobs inherit the UserID of the submitter
  - NJE & RJE jobs still require USER= + PASSWORD=

 Life of a Job 7

# Renaissance Job




 Life of a Job 8

# PROPCNTL

- PROPCNTL suppresses propagation
  - Backwards logic used
    - Resource definition in PROPCNTL = do not propagate
    - PERMITs and UACC have no meaning
  - Examples
    - PROPCNTL XYZZY - suppresses UserID XYZZY
    - PROPCNTL CICS* - suppresses UserIDs starting with CICS
    - PROPCNTL * or ** - suppresses **all** propagation

 Life of a Job 9

# JES(EARLYVERIFY) – R.I.P.

- SETROPTS JES([NO]EARLYVERIFY)
  - Added at MVS/XA 2.2 (Mid 1980's)
    - Required SAF pre-processing exit
      - Written by installation
    - Almost never used
    - Mostly implemented in other OEM security products
  - Rendered 100% inert at MVS/ESA 3.1.3 (1990)
    - Not a valid audit finding on or off

 Life of a Job 10

A job for the 90's
(and whatever that
decade after the 90's is called…)

# The Post-Modern Job



## The Post-Modern Job

- IBM added a whole slew of new job controls as of
  MVS/ESA 3.1.3 + JES2/3 SP 3.1.3 (1990)
- Security Invocations occur throughout the entire life of the job
- Life becomes much more secure… ?

## Where does a job really live?

- Where does a job really live?
  - In memory
    - during execution
  - On the spool
    - before execution
    - during execution
    - after execution
- RACF properties live in the Security Token

 Life of a Job 13

## Security Tokens (preview I)

- Security Token contains:
  - Execution USER, GROUP, NODE
  - Submitting USER, GROUP, NODE
  - POE - Point of Entry
    - JESINPUT - JES input device for a job
  - Other information

 Life of a Job 14

## Token vs. ACEE

ACEE
- Created/delete by signon
- Exists for life of session only
- Can not be copied
  - Non-movable

Token
- Created by
  - Signon (for ACEE)
  - VERIFYX
  - TokenBLD
- Exists as long as related object exists
- Can be copied

 Life of a Job 15

## Life of a Job

- Get up in morning
- Have coffee
- Take train to work
- Have coffee
- Get chewed out by boss
- Have coffee
- Take train home from work

 Life of a Job 16

## Life of a Job (Local vs NJE)

| LOCAL JOB | NJE JOB |
|---|---|
| 1. Submission | 1. Submission |
| 2. | 2. *Transmission* |
| 3. Job Validation | 3. Job Validation |
| 4. Conversion | 4. Conversion |
| 5. Execution | 5. Execution |
| 6. | 6. *Transmission* |
| 7. Output processing | 7. Output processing |

 Life of a Job 17

## Step 1 - Submission

18  Life of a Job

## Submission

- Jobs enter JES from
  - Internal Reader
  - RJE
  - Card Reader
  - NJE (foreign node's internal reader)
- Each has a different set of background information captured

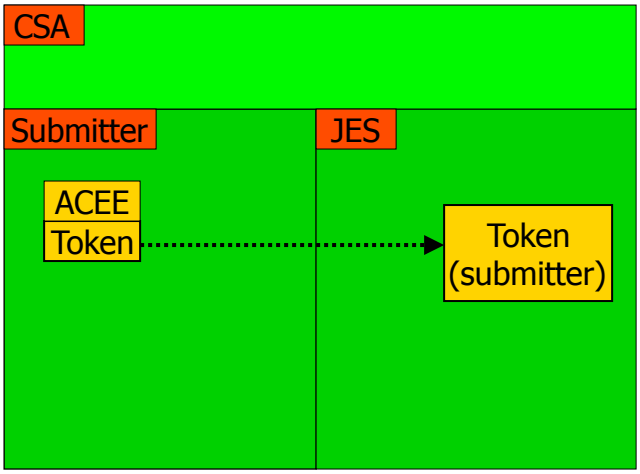


## Submission - INTRDR

- Submitter's Token captured
  - Submitter's UserID and Group can be propagated to become the execution UserID & Group
- Examples of INTRDR submissions
  - TSO Submit
  - Direct write to Internal Reader

```
//SYSUT2  DD  SYSOUT=(A,INTRDR)
```

## Submission - INTRDR



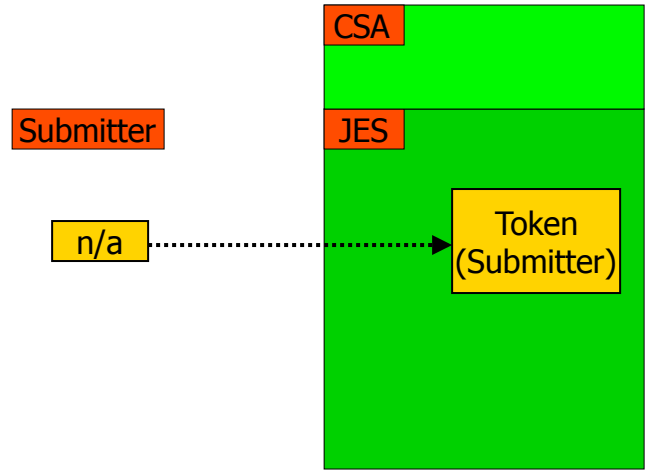

 Life of a Job 21

## Submission – RJE & READER

- RJE
  - RJE operator's Token captured
- READER
  - Card reader starter's Token captured
- RJE & READER
  - Token information never propagated to job
  - USER= & PASSWORD= required for job to run defined

 Life of a Job 22

## Submission – RJE & READER




 Life of a Job 23

## Submission - NJE

- Processing occurs at different node
  - Job could be from Internal Reader, RJE or Card reader
  - Same information captured
  - Propagation will depend upon method of submission

 Life of a Job 24

## Step 2 - Transmission



## Transmission (NJE only)

- Submitter information carried along with JOB in NJE Header
- Transferred along with job through as many nodes as it takes for job to arrive at execution node
  - No processing of job occurs at store & forward nodes

- Assign Job Number
- Assign USERID

# Step 3 – Job Validation



# Job Validation

- Occurs at execution node, on:
  - Occurs (locally) in submitter's address space
  - NJE JES3: Global
  - NJE JES2: image receiving job
- Execution job number assigned
- RACF invoked via RACROUTE REQUEST=VERIFYX

# RACROUTE VERIFYX

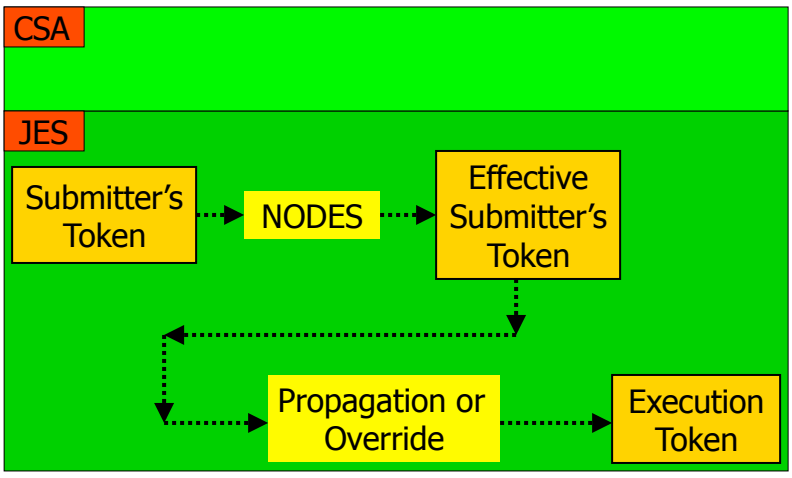
- Results in job execution security token
  - Or results in job failure
- Involves
  - RACF classes

    RACFVARS NODES
    SURROGAT JESINPUT
    PROPCNTL JESJOBS
  - SETROPTS

    JES(BATCHALLRACF)

 Life of a Job 29

# VERIFYX




 Life of a Job 30

## VERIFYX, NJE, & NODES

- NODES provides NJE UserID translation
  - Job submitter must be
    a) Valid local UserID
    b) "Undefined"
  - Job's execution UserID must be
    a) Valid local UserID
    b) "Undefined"
  - Groups must match UserIDs
  - Mismatches will flush job

## RACFVARS &RACLNDE

- Defines list of JES nodes local to this RACF
- Bypasses all NODES processing
  - If submission node is a member, then the job treated as locally submitted job
- Must only contain actual local nodes
  - Mismatches will cause failures
    - Submitting UserID must exist locally

## &RACLNDE Example

- RACF DB 1 shared by 5 JES nodes:
  - JFK, LGA, ISP, EWR, HPN

```
RDEF RACFVARS &RACLNDE          +
  ADDMEM(JFK LGA ISP EWR HPN )
```

- RACF DB 2 shared by 2 JES nodes:
  - TPA, PIE

```
RDEF RACFVARS &RACLNDE          +
  ADDMEM(TPA PIE)
```

 Life of a Job 33

## VERIFYX NODES processing

- NODES profile *node.USERJ.submitter*
  - matches
    - Submitting NODE
    - Submitting USER
  - UACC allows or denies job entry
  - Member value allows for optional local translation of foreign UserIDs

 Life of a Job 34

## VERIFYX NODES processing

- NODES profile *node.USERJ.submitter*
  - UACC:

| | |
|---|---|
| **NONE** | flush job |
| **READ** | accept job but ignore inherited user |
| **UPDATE** | accept job and user information |
| **CONTROL** | same as update, needed for jobs originating from VM systems |

 Life of a Job 35

## VERIFYX NODES processing

- NODES profile *node.USERJ.submitter*
  - ADDMEM(userid):
    - Used with UACC(UPDATE) or UACC(CONTROL)
    - Translates incoming userid to substitution value
    - Only 1 value used (do not add multiple values)
  - Example:

```
RDEF NODES TPA.USERJ.* UACC(CONTROL)
  ADDMEM(#FLTPA)
```

 Life of a Job 36

## VERIFYX NODES processing

- NODES profile *node.GROUPJ.subgroup*
  - matches
    - Submitting NODE
    - Submitting GROUP
  - Independent of "USERJ" profile
  - member value &DFLTGRP allows submitter's local default group to be used
    - Prevents failures due to group mismatches

 Life of a Job 37

## VERIFYX NODES processing

- NODES profile *node.GROUPJ.subgroup*
  - **Recommendation:**
    - Only create one profile – unless you have list-of-groups inactive:

```
RDEF NODES *.GROUP%.* UACC(READ)
  ADDMEM(&DFLTGRP)
```

 Life of a Job 38

## Who's on First?

- Actual Submitter
  - USER that performed the job submission
- Effective Submitter
  - Usually the Actual Submitter
  - Used during Job Validation
  - Result of NODES translation
    - Discarded after VERIFYX



## Who's on Second?

- Execution User
  - USER associated with job execution
  - Precedence
    1. USER= on job card
       - With or without PASSWORD=
    2. "Effective Job Submitter"
       - Result of NODES or actual submitter (local)
    3. "Undefined"

## Who's on Second?

a) USER= + PASSWORD=
   - Password evaluated
     - Invalid UserID or invalid password – flushes job

b) USER= without PASSWORD=
   - Validated by SURROGAT *userid.SUBMIT* profiles
     - Submitter not authorized - flushes job

c) Propagation
   - Job inherits "Effective Job Submitter"
     - PROPCNTL suppresses propagation (undefined)

 Life of a Job 41

## Who's on, period?

- If no defined user, then if
  - JES(NOBATCHALLRACF)
    - Job passes VERIFYX as undefined
    - Displayed value from JES(UNDEFINEDUSER( ))
      - Default is ++++++++
  - JES(BATCHALLRACF)
    - Job flushed

 Life of a Job 42

## POE, Edgar Allan

- JESINPUT profiles (Point Of Entry of job)
  - Authorize entry for all jobs and sysout
  - Resource name = JES device name
    - INTRDR
    - Rn.RDn (RJE)
    - adjacent-node-name (NJE)
    - OFFn.RDn (Spool offload)
  - Failure flushes job

 Life of a Job 43

## JESJOBS

- JESJOBS SUBMIT.node.jobname.userid
- Authorizes combination of jobname with execution UserID
  - Authorized against "Effective Job Submitter"
  - Failure flushes job
  - Active alternative to PROPCNTL
    a) JESJOBS - Direct violation against submitter
    b) PROPCNTL – Job fails due to undefined

 Life of a Job 44

## El Grande VERIFYX Summary

- &RACLNDE / NODES
- PROPCNTL / SURROGAT / Password
- BATCHALLRACF
- JESINPUT
- JESJOBS

 Life of a Job 45

- Process JCL

## Step 4 – Conversion

46  Life of a Job

## Conversion

- Occurs at execution node, on:
  - JES3: Global
  - JES2:
    - /*JOBPARM SYSAFF=id image
    - image receiving job
- Occurs under User's security environment
  - RACROUTE VERIFY issued using token



## Conversion

- Involves the following RACF classes:
  - DATASET
    - if private proclibs used for job
- Additional checking available via JES exits for:
  - JCL operands
  - Account validation

## Conversion

- If system commands present in jobstream…
  - RACF OPERCMDS class used to validate command authority
    // D A,L
    // ACTIVATE …
  - Commands execute at this time



- Run job, run!

## Step 5 – Execution

## Execution (Initiation)

- Job selected by JES for initiation
- SMS preprocessing may cause additional RACROUTE VERIFY prior to normal initiation
- RACROUTE VERIFY issued at actual job initiation

 Life of a Job 51

## Execution

- SYSOUT created by job is validated via WRITER, including
  - local SYSOUT
  - NJE SYSOUT
  - new jobs submitted by executing job
- WRITER failure
  - causes routing to fail, but does not purge

 Life of a Job 52

- Roam where you want to …

## Step 6 – Transmission



## SYSOUT Transmission

- Routed output
  - joblets have execution token of job
- Are reprocessed by VERIFYX at destination node (when not local)
- ➔ More NODES processing

- Do it to me one more time…

## Step 7 – Output Processing

## Who's on First, again…

- Joblets left as is when execution node is in the output node's
  RACFVARS &RACLNDE
- Otherwise NODES processing occurs

## Return of NODES

- NODES profile
  *exec-node.USERS.exec-userid*
  - matches
    - Execution NODE
    - Execution USER
  - UACC allows or denies sysout receipt
  - member value allows for local translation of foreign userids, or reversion to original userid (&SUSER)

 Life of a Job 57

## Return of NODES

- NODES profile
  *exec-node.GROUPS.exec-userid*
  - matches
    - Execution NODE
    - Execution GROUP
  - Best handled by same profile as GROUPJ:

RDEF NODES *.GROUP%.* UACC(READ)
ADDMEM(&DFLTGRP)

 Life of a Job 58

## Son of NODES

- Sysout translation failure causes sysout to have unassigned userid.
  - Sysout not normally purged
  - Can be purged because of JESINPUT failure
    - Job JCL and Job sysout processed separately.

 Life of a Job 59

- The "Afterlife"

## L'Après vie

60  Life of a Job

## Printing

- Accessibility to print device authorized through WRITER class
  - may be ignored by OEM writers



## Viewing Jobs

- JESSPOOL class is used to validate
  - viewing
  - purging
- JESSPOOL only affects spool files not owned by your own userid
  - Mixed UserID situation may occurs under IMS MPP
    - Job belongs to MPP
    - Sysout created by end user not MPP

"Do your own thing"

# Customization

# "Danger Will Robinson!"

- VERIFY and VERIFYX both invoke:
  - SAF Router Pre-processing exit
  - RACINIT Pre-processing exit
  - RACINIT Post-processing exit
- Therefore
  - caution is advised in trying to change the current UserID, it may have strange or even no effect

## Good Ideas

- Using exit(s) to:
  - Force assign UserID to READER or RJE job
  - Disallow PASSWORD= equal on job card
  - Validate accounting information
  - Validate JCL operands during conversion

 Life of a Job 65

Thanks for coming.

## Questions?

66  Life of a Job