How to Get Full Security from Security Software and Tape Management Software Together

Monday, August 22, 2005

Session 1714 1:30

Stu Henderson (stu@stuhenderson.com)
Russell Witt (russell.witt@ca.com)

Abstract

- One of the major weaknesses in mainframe security at most installations is security for tape datasets. Whether you have RACF, ACF2, or TopSecret for your security software, tape security is complicated by several issues.
- In this session Russell and Stu describe the issues that make tape security difficult, and show you practical ways to address them. Whatever your security software, and whatever your tape management software, you will learn to integrate the two to strengthen your installation’s data protection
- Our approach was to lay out the issues and review possible approaches with representatives of each of the tape management products.

Agenda

- Introduction and Background
- Open/Close/EOV Issues
- Our Recommendations
- Summary and Call to Action

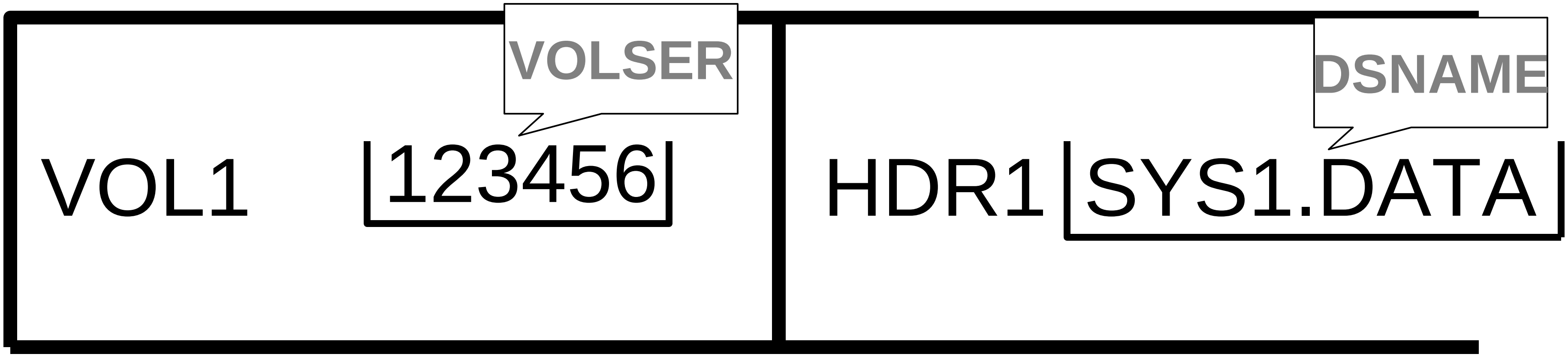
Introduction and Background

- Mainframe security software originally checked Userids/Passwords and accesses to Disk Datasets, based on the DSNAME of each Dataset
- Vendors then added protection of tape Datasets, first based on tape volume. When the number of tapes grew, this became impractical
- Later they added protection based on the DSNAME of each tape dataset This was still not sufficient, so we turn to TMS (Tape Management Software)

Mainframe System Software Has Tape Checks Not Found on Other Platforms

- The first two records on most tapes are:
  - The Volume Label, 80 characters long, with the unique VOLSER number that identifies that tape
  - The Header Label, also 80 characters, with the DSNAME of the First Dataset on the tape (just the rightmost 17 characters)

Mainframe System Software Has Tape Checks Not Found on Other Platforms



VOLSER

VOL1 123456

DSNAME

HDR1 SYS1.DATA

<-80 Character Volume Label-> <-80 Character Header Label->

Later, When Someone Tries to Read the Tape the System Makes 4 Checks

- Check VOLSER in VOL1 Label
- Check DSNAME in HDR1 Label
- Call Security Software to Check Access by DSNAME from the JCL.
- Give Control to Tape Management Software, full 44-character DSN is recorded or validated.

These Checks Apply Also to Virtual Tapes

- **A Virtual Tape is one that appears like a real tape, but may be on any of several types of medium, including telecommunications links**

The Most Common Tape Management Software (TMS) Packages Include:

- **BrightStor CA-1 (Formerly TMS or UCC1)**
- **BrightStor CA-Dynam/TLMS**
- **IBM's DFSMSrmm**
- **BMC's CONTROL-M/Tape (Formerly CONTROL-T)**
- **ASG's ZARA**

All of These TMS's:

- Keep info about each tape volume (that is, Cartridge) in a database on Disk
- Can call SAF for their own functions
- Gets control from Open, from Close, from EOV (End of Volume)
- Defines the range of tape VOLSERs considered to be In-House

Open/Close/EOV Issues

- 17 Character DSNAME
- Bypass Tape Management Software
- BLP (Bypass Label Processing)
- Foreign Tapes
- 2nd File Read Backward
- Residual Data

For Each Issue, You Might Use SAF and/or TMS, Depending On:

- **Is the Tape In-House**
- **Is the Tape Foreign (received from another organization, likely with different standards for VOLSER numbers and DSNAMES), likely ID'd as EXPDT=98000**
- **Is the tape Sent-Out (and therefore not protected by our SAF or TMS)**

SAF Considerations

- **SAF software can control access by VOLSER (RACF: TAPEVOL; ACF2: SECVOLS and RESVOLs; TSS: VOLUME resource class) – OR –**
- **SAF Software can control access by DSN (SETROPTS TAPEDSN option for RACF, GSO OPTS TAPEDSN for ACF2 or TAPE(DSNAME) for Top Secret)**
- **RACF – TVTOC – Tracks all files on tape volumes**
  - **Most Shops Don't Use Because:**

    Limits on Numbers of Volumes and DSNAMES

    High administration and system overhead

    Duplication with Tape Management System

SAF Considerations (cont'd)

- For good security, SAF software should be set to fail requests for DSNAMEs with no matching rules (RACF: PROTECTALL; ACF2: default; TopSecret: DEFPROT)
- This may lead to requests to bypass security for users processing foreign tapes (which have non-standard DSNAMES)
- Do we really want to give this out?

SAF Considerations (cont'd)

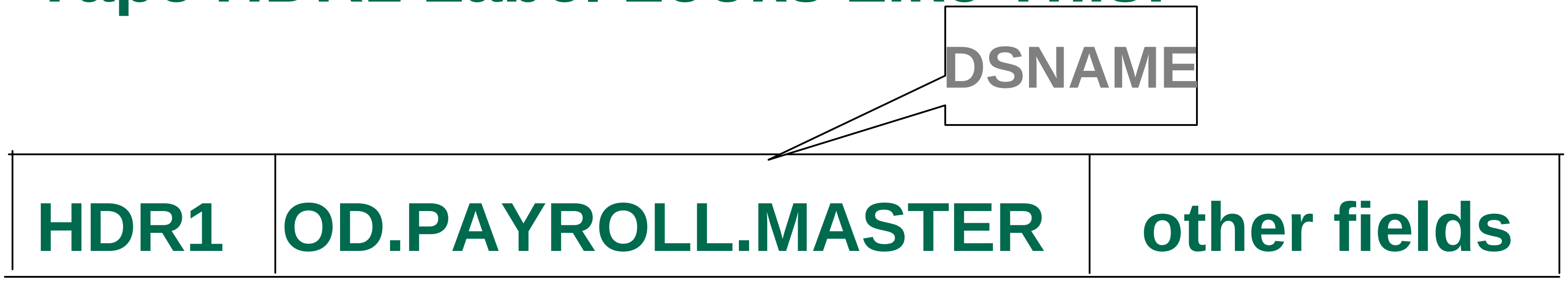
- Your TMS can solve this by recognizing which tapes are Foreign and which are In-House
- Some TMS can make the SAF call on the DSNAME themselves. The TMS can then decide whether to fail the request if no matching rule is found, based on whether the tape is In-House or Foreign.

17 Character Dsname Issue

- Since the label carries only the right-most 17 characters, I can lie to the system by giving a fake DSNAME that matches the right-most 17, but has my USERID as the High Level Qualifer (HLQ).
- Need to carry the full 44 character DSNAME somewhere. The TMS can do this, and then insure what is in the JCL matches what is recorded in its database.

17 Character Dsname Issue (cont.)

- **JCL to create tape dataset - DSN=PROD.PAYROLL.MASTER**
- **Tape HDR1 Label Looks Like This:**



DSNAME

HDR1	OD.PAYROLL.MASTER	other fields

- **JCL to read tape dataset – w/o TMS DSN=userid.OD.PAYROLL.MASTER**

17 Character Dsname Issue (cont.)

- Tape Management will save the original file-name within it's own database during creation.
- Tape Management Software will validate the full 44 character DSN (by matching the original full 44 character DSN stored in its database with what is in the JCL) when read for input.
- Some TMS have an option to make SAF calls in the DATASET class, using the full 44 character dsname during OPEN processing in addition to the normal SAF calls made by OPEN processing.

Bypass Tape Management Software

- Will allow anyone to “trick” normal OPEN processing with wrong dsname
- How to bypass TMS?
  - JCL ➔ EXPDT=98000
  - JCL ➔ ACCODE=XCANORES
  - OS ➔ shutdown TMS
- Insure that ALL are controlled via external security controls (SAF)

Bypass Tape Management Software (cont.)

- BrightStor CA-1
  - Option → FUNC   Y or E
  - Class → CA@APE
  - Resources →FORRES or FORNORES
  - Enhanced resource→FORres/nores.UCB*nnnn*.V*volser*
- BrightStor CA-Dynam/TLMS
  - Option → FORSEC
  - Class → CA@APE
  - Resources →FORRES or FORNORES

Bypass Tape Management Software (cont.)

- DFSMSrmm
  - Class → FACILITY
  - STGADMIN.EDG.IGNORE.TAPE.RMM.*volser*
  - STGADMIN.EDG.IGNORE.TAPE.NORMM.*volser*
- CONTROL-M/Tape
  - Class → FACILITY
  - Resource → $$CTTBYPASS.*qname.volser*
- ZARA
  - Option → 98000
  - Class → T$SYSTEM
  - Resource → BYPASS.loc.lbl.typ

Shutdown Tape Management Software

- If TMS is not active, 17-character only dsname checking is performed
- No prevention of overwriting not-scratched data
- No tracking of files created for off-site movement

Shutdown Tape Management Software (cont.)

- DFSMSrmm
  - Class → FACILITY
  - Resource → STGADMIN.EDG.RESET.SSI
- CONTROL-M/Tape
  - Class →FACILITY
  - Resource → $$CTTINI.qname

Shutdown Tape Management Software (cont.)

- BrightStor CA-1
  - Class ➔ CA@APE
  - Resource ➔ REINIT or BATCH or DEACT
- ZARA
  - You must respond to the following WTOR

TXIT04A ZARA UNAVAILABLE FOR TAPE USE, Unit=unit Job=jjjjjjjj Retry or Abend?

BLP (Bypass Label Processing) Issue

- **If I Can say LABEL=(2,BLP) on a DD Card, I can bypass the security for every tape dataset**
- **Originally JES Controlled Who Can BLP**
  - **By type (STC, TSO, batch-job by class)**
  - **Difficult to tell why a tape is being rejected**
- **Now the security software can control it, and also some TMS can. TMS however can distinguish foreign tapes.**

BLP Issue (cont.)

- BrightStor CA-1
  - Option → FUNC YES or Enhanced
  - Resources → BLPRES or BLPNORES
  - Enhanced resources → BLPres/nores.UCB*nnnn*.V*volser*
- BrightStor CA-Dynam/TLMS
  - Option → BLPSEC
  - Resources → BLPRES or BLPNORES

BLP Issue (cont.)

- DFSMSrmm
  - Option → BLP (RMM/NORMM)
- CONTROL-M/Tape
  - Option → TBLPCHK
  - Class → FACILITY
  - Resources → $$CTTBLP.*qname.volser*
- ZARA
  - Option → SAF BLP
  - Class → T$SYSTEM
  - Resource → BLP

Foreign Tapes Issue

- A Foreign Tape is One From Outside Your Organization.
- The dataset names used probably do not match your internal naming conventions
- If your External Security System does the SAF call during ALL OPEN processing, then foreign tapes are a problem

Foreign Tapes Issue (cont.)

- You can grant access to the specific foreign volume, this will allow access without a dataset name check.
  - Make sure the volume is not a duplicate with any in-house volumes
  - Delete the profile when the volume is returned or no longer needed.
- You can create an exit for your External Security System to allow access for foreign tapes
  - You will need to interface to your TMS from the exit.

Foreign Tapes Issue (cont.)

- BrightStor CA-1
  - Options ➔ OCEOV – YES
    CATSEC – YES or BYP
    FORNDSN – OUTPUT

  Note: These options will duplicate all calls that are invoked with TAPEDSN, except for foreign tapes being read for input. This gives you the option of turning off TAPEDSN.

2nd File Read Backward Issue

- If there are two files on one tape cartridge, and you let me create or read the second one, then I can read the first one by issuing the command backward-space-file.
- Security software cannot prevent this
- Tape Mgt. Software can control what secondary files are stacked upon the tape

2nd File Read Backward Issue (cont.)

- RACF – TVTOC will keep track of ALL datasets on the volume.
    - High system overhead
    - Creation of file 9 means 8 extra SAF checks
    - Low limits on volume-count and file-count
- BrightStor CA-1
    - Option → DSNB
    - Will check file-1 whenever file-n is created or read

2nd File Read Backward Issue (cont.)

- CONTROL-M/Tape
  - OPTION ➔ DO STKRULE NOTWITH JOB jobname
    ➔ DO STKRULE NOTWITH DSN dsname
- ZARA –
  - OPTION ➔ DSN ALL / 1ST

Residual Data Issue

- When a tape dataset’s retention period has been reached, the tape can be returned to the scratch pool
- Whoever next uses that tape can browse the data on it (similar to residual data on disk)
- Two Situations: tape kept in-house and tape shipped outside of your company

Residual Data Issue (cont.)

- Tapes sent to other companies are the most at-risk
  - Encrypt in case the tape is stolen or lost from the delivery truck
  - Copy data to a never-been-used cartridge
  - Copy data to a fully degaussed or software erased cartridge
  - Erase residual data on existing tape volumes

Residual Data Issue (cont.)

- Tapes kept in-house are also at risk
- Use TMS to prevent tapes in scratch status from being called by specific volser
- Use sub-pools to prevent mixing of different security related groups (a sub-pool is a group of tapes to be treated the same, for example, all scratch, or all production payroll tapes)

Residual Data Issue (cont.)

- BrightStor CA-1
  - Utility – TMSTPPRO ➔ Erase and re-initialize
  - Utility – CTSDEU ➔ Erase residual data on active volume or erase entire tape and reinitialize
- BrightStor CA-Dynam/TLMS
  - Utility – CTSDEU ➔ Erase residual data on active volume or erase entire tape and reinitialize

Residual Data Issue (cont.)

- DFSMSrmm
  - Will not allow a SCRATCH tape to be called by volser
  - Option → SECCLS (ERASE)
  - Utility → EDGINERS (erase and reinitialize)
- CONTROL-M/Tape
  - Option → SCRPROT = Y (to prevent a scratch tape from being called by specific volser)
  - Utility – CTTTPI with a function of TAPERAS

3) Our Recommendations (in Order):

- DSN checking done at OPEN time
- Control Who Can Bypass TMS (EXPDT=98000)
- Control Who Can Use BLP
- Control Who Can Shutdown Your TMS
- Protect Residual Data on Sent-Out Tapes, then on In-House Tapes
- Control 2nd File Read Backward

Summary and Call to Action

- Following the steps laid out above will improve the quality of your security
- If you don't make this happen, then who will?
- We may do a follow-up session with details on more software, and on controlling the tape library functions. would you like that? -- Answer on evaluation

Special Thanks

- These wizards gave generously of their time and expertise for this presentation and we owe them our thanks
  - Mike Wood of IBM (DFSMSrmm)
  - Noam Herzenstein of BMC (CONTROL-M/Tape)
  - Bill Csorba of ASG (ZARA)
- Stu and Russell are still responsible for any errors

Questions ???

? ? ? ? ? ? ? ?