How to Go About Setting Mainframe Security Options

Stu Henderson
5702 Newington Road
Bethesda, MD 20816

stu@stuhenderson.com
www.stuhenderson.com
(301) 229-7187

ABSTRACT

If you don't think that checklists are the complete answer to setting security options in RACF, ACF2, or TopSecret, this session will show you practical approaches to making your own decisions and making them part of your own standards and policies. Mainframe security administrators and auditors will benefit from seeing the thought process behind effective decision making and standards development.

While much of this presentation is based on RACF settings, ACF2 and TopSecret settings are covered as well. Stu has decades of experience as a security administrator, system programmer, and auditor, and has seen (and made) his share of mistakes in all three roles. In this presentation he shares what he has learned about the process of decision making for security options, lessons that make life easier and security more reliable.

This presentation won't attempt to tell you how every setting should be set; it will show you how to think about them for yourself.

Agenda

1. Introduction

2. Our Approach

3. Examples

4. Call to Action

Appendix: For More Info

RACF, ACF2, or TopSecret

How do we go about setting the options? Several approaches:

- Checklists like the STIGs, 800-30, NewEra Ebook (see links at presentation end)
- Whatever the sysprog says
- Auditors' checklists
- Vendor checklists

Today's Approach

Based on:

- Risk assessments
- Laws, regulations, standards
- So what?

To Learn the Options

- For RACF: **SETR LIST**
- For ACF2, **SHOW ALL**
- For TopSecret:

TSS MODIFY(STATUS)

What's Important Here:

- The process for deciding
- Who is involved.
- Not the actual settings themselves, which may vary among data centers

Approach

- For a few example options, we'll show our process for deciding
- Not every option
- Not every consideration
- Auditor or administrator, you can adopt the process as you see fit

Approach: Our Process

- What could happen?
- What is the risk?
- What regulations/standards apply?
- Who knows?

The Example Options

- Protect all batch jobs
- Protect all datasets
- Residual data on disk

Protect All Batch Jobs

- What could happen?
- What is the risk?
- What regulations/standards apply?
- Who knows?

Protect All Batch Jobs

To ensure every batch job has a valid userid:

- In RACF, two options
  - BATCHALLRACF (batch jobs)
  - XBMALLRACF (joblets)

Protect All Batch Jobs

What could happen if BATCHALLRACF not active?

- Batch jobs with no userid, submitted from: RJE, NJE, FTP, CICS, MQ, TSO, started tasks
- Could then access any dataset or resource with open default access
- Or someone could run a service bureau on the company's mainframe

Protect All Batch Jobs

On the other hand, not a problem if:

- We control every path in: RJE, NJE, FTP, every started task, CICS, IMS, MQ, …

- Default accesses all NONE

Protect All Batch Jobs

Easier to control the risk by just setting one option: BATCHALLRACF

- Easier to know you're secure
- Easier for auditor to say it's secure

Protect All Batch Jobs

A second option: XBMALLRACF

- Used only with the JES eXecution Batch Monitor
- Which is rarely used (multiple compiles in university)
- If no eXecution Batch Monitor, it makes no difference, but doesn't hurt either

Protect All Batch Jobs

Perhaps BATCHALLRACF is worth spending security and audit resources on, but XBMALLRACF much less so.

Our point is that:

- Someone else's checklist should be much less important than your understanding of the risk

Protect All Batch Jobs

In ACF2

- If in ABORT mode, then every batch job must have a valid userid
- However DFTLID (default logonid) option specifies userid to be used for any batch job without its own userid
- Depending on this setting, the risk assessment is similar to that in RACF.

Protect All Batch Jobs

In TopSecret

- Batch jobs are controlled through the BATCH FACILITY
- However the DEFACID option can specify a default userid for batch
- The risk assessment is similar to that in RACF

Protect All Batch Jobs

- Whatever your security software, you want to know if a batch job can execute without having a valid userid
- If so, is there any risk?
- Our point again is that someone else's checklist should be much less important than your understanding of the risk

Protect All Datasets

- For RACF, we have a switch to force all datasets to be protected: PROTECTALL
- Should it be active?
- We'll take the same approach
- Then look at ACF2, and TopSecret

Protect All Datasets

- What could happen?
- What is the risk?
- What regulations/standards apply?
- Who knows?

Protect All Datasets

The risk:

- Without PROTECTALL, users could create datasets with non-standard dsnames
- Difficult to tell from the dsname what it is
- Non-standard dsname in production JCL leaves production dataset unprotected

Protect All Datasets

PROTECTALL is not difficult to implement:

- WARNING mode

- Control of High Level Qualifiers

Again: The thought process is more important here than how you set the option

Protect All Datasets

For ACF2, if MODE is ABORT, it's like PROTECTALL, but:

- ACF2 lets you protect datasets by dsname, or by volume, depending on the SECVOLS and RESVOLS options
- If a disk pack or tape volume on neither list, datasets are not protected
- Again, the thought process is more important than specific settings

Protect All Datasets

For TopSecret, if MODE is FAIL, it's like PROTECTALL, but

- TopSecret allows protection by volume or by dsname

Protect All Datasets

- If permission is given by the volume, dataset rules aren't checked

- What do you see as the risk?

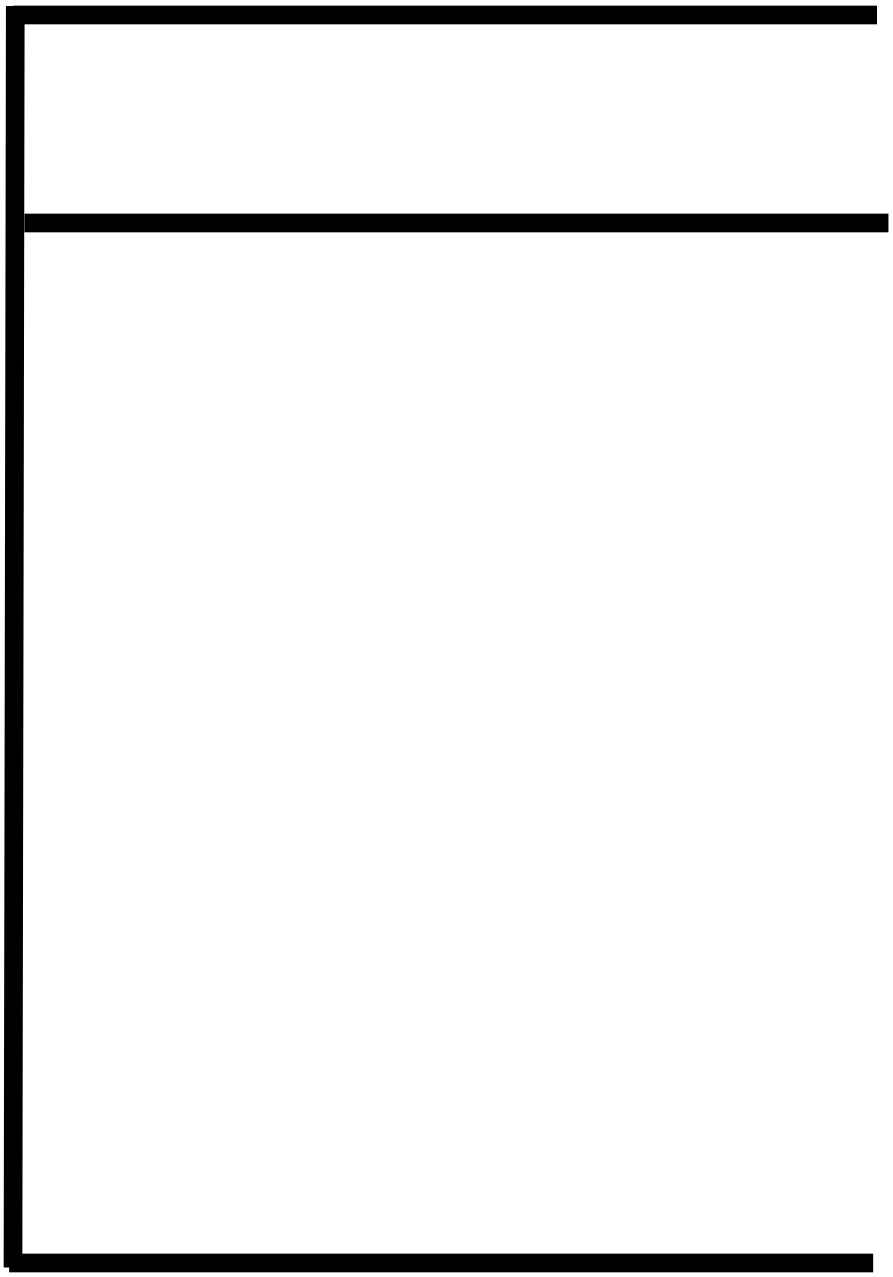
- Again, the thought process is more important than specific settings

Residual Data on Disk

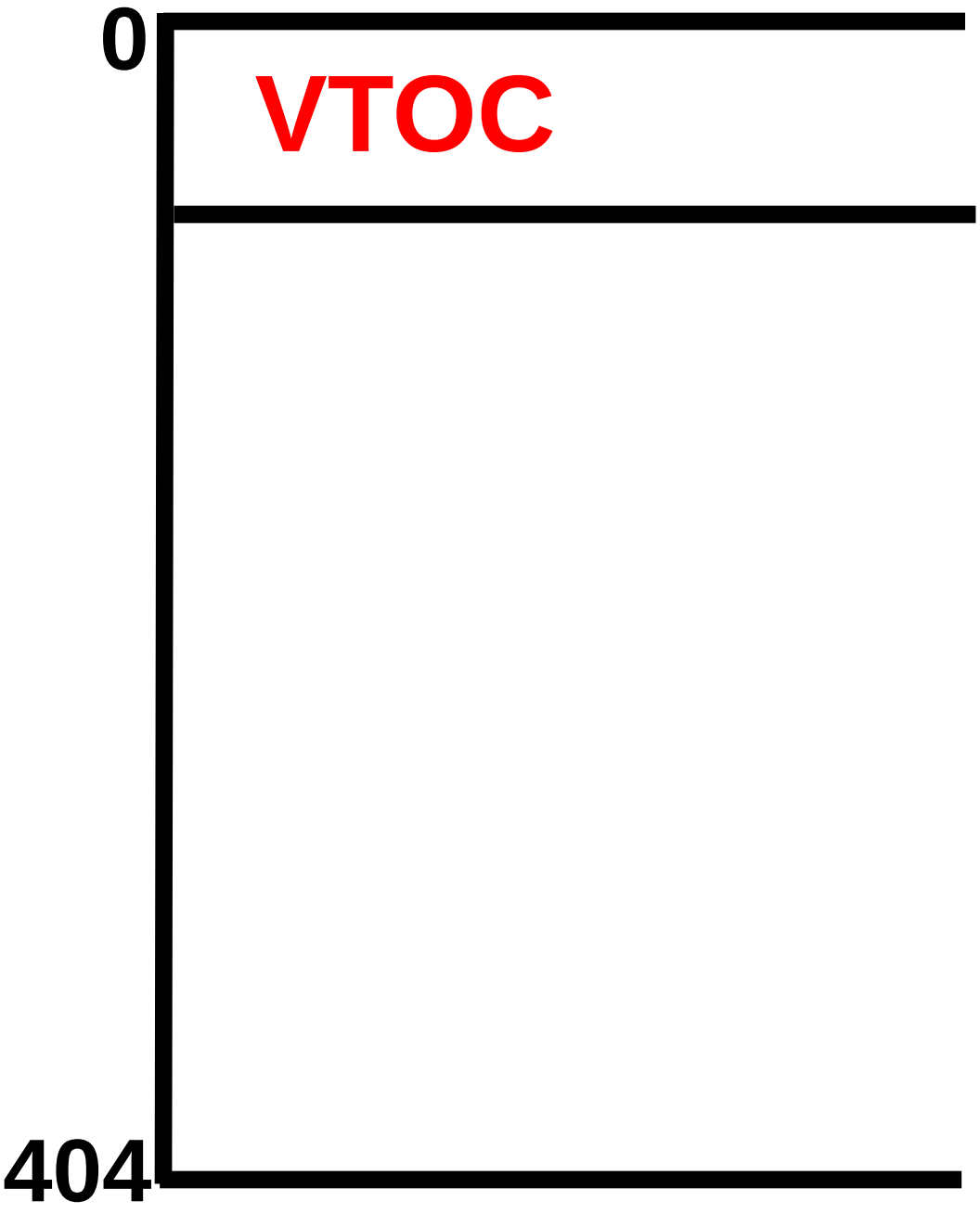
- We'll start by explaining what residual data is

- Then address the risk in each of RACF, ACF2, and TopSecret

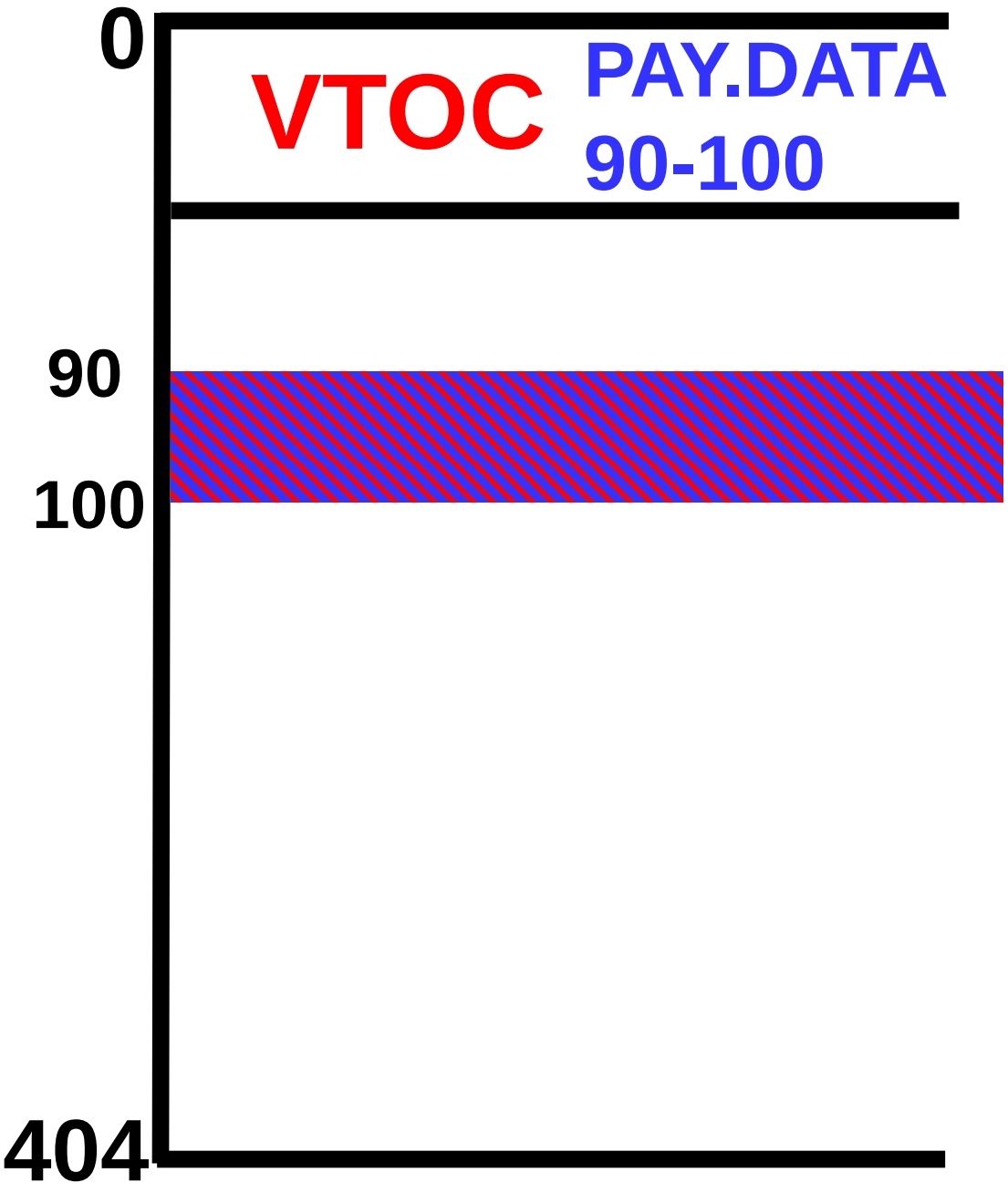
Residual Data on Disk



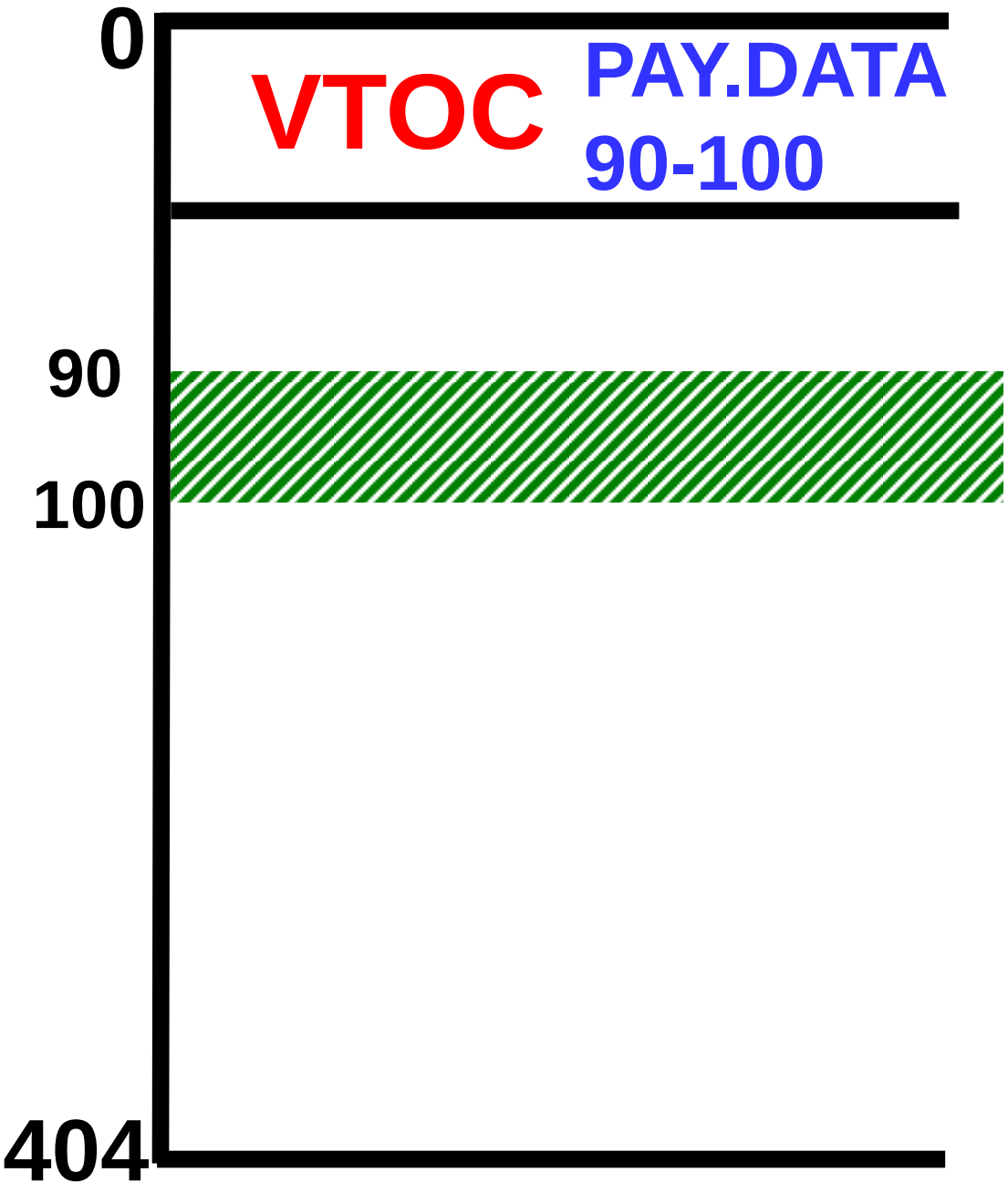
A Disk Drive



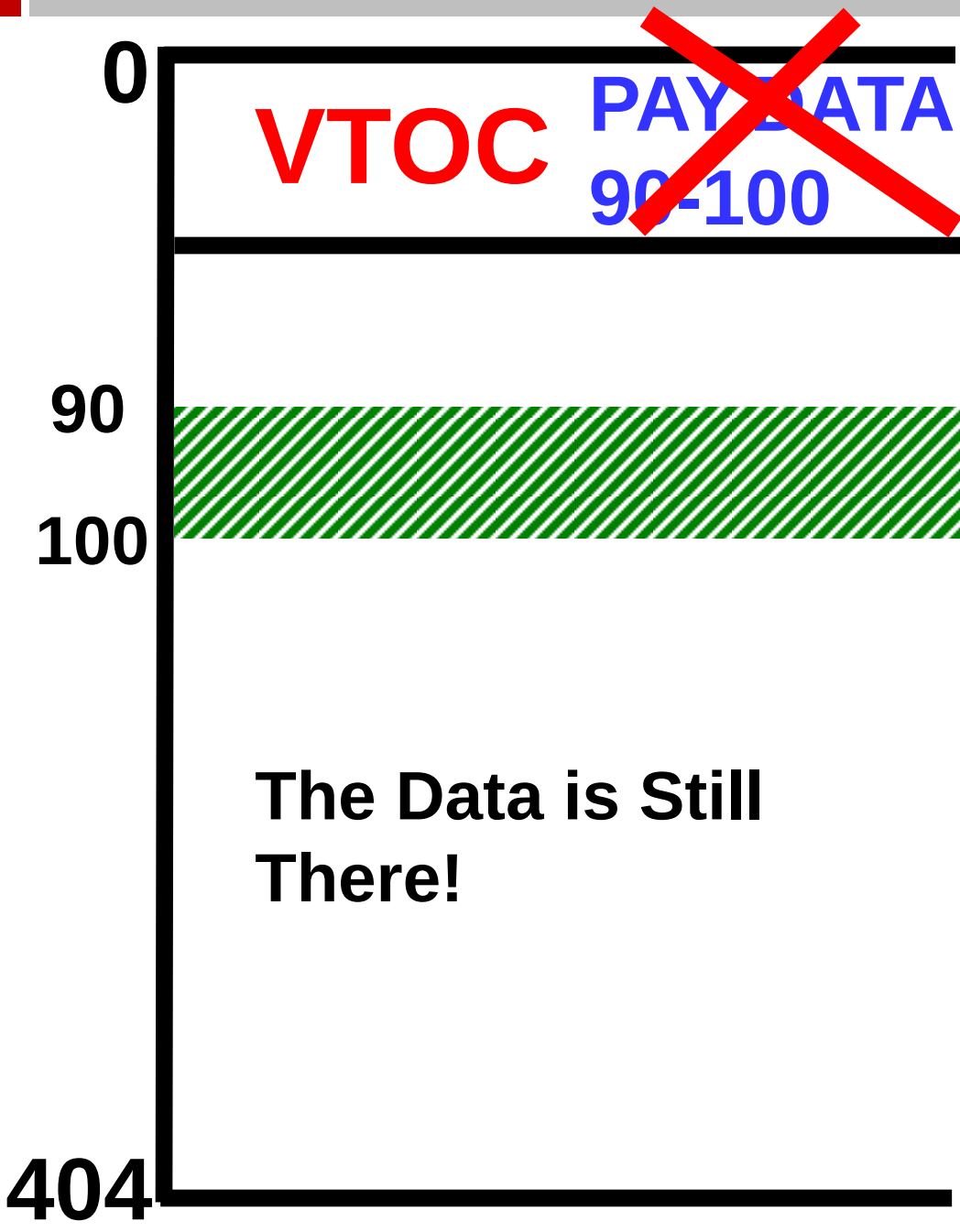
Residual Data on Disk



Residual Data on Disk



Residual Data on Disk



Residual Data on Disk

- Any TSO user can read sensitive residual data, deliberately or accidently

- By allocating a dataset on that part of the disk drive and then reading the data there.

Residual Data on Disk

IBM points out in the Security Server RACF System Programmer's Guide Version 2 Release 1 that"

"This type of attack requires no exotic tools or insider knowledge and can be done quite easily using JCL and an IBM-provided utility such as IEBGENER."

Residual Data on Disk

- RACF has an option named EOS ("**Erase On Scratch**") that obliterates disk data when a dataset is erased.

- ACF2 and TopSecret provide the same function with an option they call **AUTOERASE**.

- So how do you decide whether to implement this, and if so, to which datasets?

Residual Data on Disk

- System programmers may believe that this option has a serious performance problem (since fixed, please see Cheryl Watson's newsletter)

- Does the security administrator know what laws and regulations apply?

- Do your Legal and Compliance staff know?

For More Information

- Cheryl Watson's Tuning newsletter documents some amazing improvements in Erase On Scratch (AUTOERASE) performance with z/OS 2.1, especially with one particular APAR. She strongly recommends re-visiting whether you use EOS or not, given these improvements. She gives an amazing amount of hard, detailed measurements, backed with clear, detailed technical explanations. More in Appendix.

Residual Data on Disk

The decision whether to implement this was likely made in one of three ways:

- No one considered ("Not my job")
- The sysprog said "Don't"
- The sysprog, Legal, Compliance, application owner, and secadmin evaluated the risk together.

Residual Data on Disk

Often neither the secadmin nor the IS auditor knows all the disciplines needed to understand the risk.

Who knows?

What's Important Here:

- The process for deciding
- Who is involved
- Not the actual settings themselves

Imagine Two Scenarios

First scenario:

- Security administrator sets options
- With input and occasional vetoes from sysprog
- No baseline, written standard of how the options should be set
- It's all in the security admin's head

Imagine Two Scenarios

Second scenario:

- Policy assigns responsibility for option setting roles: application owners, sysprogs, security admins, Legal, other
- Result is summarized in baseline document
- Auditors use the baseline as a standard

Imagine Two Scenarios

First scenario could result in:

- Audit finding that there is no standard to audit against and that the organization doesn't understand associated risks

- Auditor using a "one size fits all" checklist as the standard to compare against

Call to Action

- We've shown you a thought process and illustrated with a few examples
- You can apply the process to all of your mainframe security options
- If you don't, someone else will try to tell you to follow their checklist
- If you do, you'll have better security and easier audits

4 Basic Questions on Risk

- What could go wrong?
- What regulations/standards apply?
- Who decides and how?
- How easy to reduce risk?

Basic Concepts

- First, understand the risk
- Defense in depth
- Low overhead defense
- Easier to sleep well

Basic Concepts

- Make someone responsible

- Some large exposures result from two smaller ones together

- Preventive controls better than detective or corrective

More Areas to Address

- USS (aka OMVS) Security
- TCP/IP Security
- Policy Agent Software Tool
- Batch job submission with different userid
- All the resource classes

More Areas to Address

- Privileges on userids
- Passwords
- All the options in SETR LIST, SHOW ALL, TSS MODIFY(STATUS)

See the appendix to New Era's book on SETR options for more examples

For More Information

- New Era's ebook on RACF Options

"***AE2 - z/Auditing Essentials - Volume 2 - The Taming of SETROPTS***"

http://www.newera-info.com/AE.html

For More Information

Other volumes in the series:

- ***AE1 - z/Auditing Essentials - Volume 1 - zEnterprise Hardware*** - An Introduction for Auditors
- ***CICS Essentials - Auditing CICS*** - A Beginner's Guide
- ***CICS Best Practices***
- ***CICS Alphabet SoupWhat's New in z/OS V2R1***
- ***What's New in z/OS V2R2***

For More Information

- The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes:

https://web.nvd.nist.gov/view/ncp/repository

- Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53):

http://csrc.nist.gov/publications/PubsSPs.html#800-53

For More Information

- Newsletters ("***RACF User News***" and "***Mainframe Audit News***") at

www.stuhenderson.com/Newsletters-Archive.html

- Handouts from meetings of the New York RACF User Group: (www.nyrug.stuhenderson.com/handouts.HTM)

For More Information

- **Frank Kyne performed erase-on-scratch testing that is documented in Cheryl Watson's "TUNING Letter - 2015 No. 1":**
  - Allocated data sets of 1, 100, 255, 25600, and 63000 tracks
  - Ran a separate job to delete each data set, varying erase-on-scratch on and off, on z/OS V1R13 and z/OS V2R1
- **Frank's results:**
  - Small reduction in elapsed time and EXCP counts for the smaller data set sizes (1, 100, 255)
  - Large reduction in elapsed time and EXCP counts for the larger data sets
    - For the 63,000 track data set, EXCPs dropped from 63,007 to 263
    - Elapsed times decrease between 1/3 and 2/3
- **Once you are on z/OS V2R1, perhaps it's time to revisit erase-on-scratch!**

For More Information

- To subscribe or to see a sample issue, of Cheryl Watson's newsletter:

http://www.watsonwalker.com/sampleissues.html

Thanks for Your Kind Attention.

Questions to Stu Henderson

(301) 229-7187

stu@stuhenderson.com