MANEWS 14

the Mainframe Audit News

March, 2010 Issue Number 14

==========
==========

Table of Contents

This issue of the MAN describes how to think about passwords in an audit. It then shows you how to think about them more deeply.

==========
==========

1) How to Think About Passwords

Passwords are our most basic way of proving who we are to a computer. By implication, this is also how we control who can use our computer. Your audit methodology may have steps to examine the controls over password length and content. (The longer a password is, and the more possible values for each character, then the harder it is for a hacker to guess it.)

Your audit program may ask you to "***Verify that passwords have a minimum length of six characters and must contain at least one number and at least one letter***."

Since all signons should be processed by the security software (always one of: RACF, ACF2, or TopSecret), you should get the password rules from the security software and compare them to whatever the standard is. You will also want to learn about any password processing exits. These are programs added to the security software which can further restrict password length and content.

For **RACF**, you would look at the SETR LIST and DSMON reports. [For help in interpreting these two listings, please go to www.stuhenderson.com and click on ARTICLES.] For **ACF2**, look at the SHOW ALL output. For **TopSecret**, look at the TSS MODIFY(STATUS) output. For ACF2 and TopSecret, there may also be a list of reserved words which cannot be used as passwords.

You might also inquire whether there is "two-factor authentication". This is a requirement that users prove in two different ways who they are. For example one way might be a password (something they know). But they might also be required to type in a unique, changing, random number provide by a hand-held token, the second factor.

The two factors should be of different types (something you know, something you hold, something you are [biometrics]) to provide the most effective protection.

But if your audit mechanically compares actual password rules for length and content to some standard, you may miss the point: **how well do passwords prevent unauthorized users from using the system, how well do they prevent spoofing of userids**?

==========
==========

2) How to Think Deeply About Passwords

If you want to do a more thorough job, you will want evaluate how well passwords protect the system. That is, how well do they prevent people from using the computer without being authorized, and how well do they prevent someone from assuming someone else's identity when using the computer. (How does this relate to the financial control objectives?) This may turn out to be more important than whether the minimum password length is 6 or 7.

Here are some further questions you might investigate in your audit:

- What paths into the system don't use the security software?
- Are password rules so complex that they weaken security?
- Are password phrases and/or mixed case allowed?
- What do password reset patterns tell you?
- How can log data reveal passwords?
- So what's the real point about passwords?

What Paths into the System Don't Use the Security Software?

Systems with z/OS have several prefined paths into the system, and several places where additional ones can be added. If there is a path into the system which doesn't call the security software to verify userids and passwords (For example, it may have its own hard-coded list of userids and passwords.), this may represent the start of an audit finding. The risk occurs when for example a user is fired for dishonesty. His userid in the security software would be deleted, but he can still access the system through one of these uncontrolled paths, using the hard-coded userid and password. You then might have a disgruntled former employee working for the competition who can get into your system, while you think you've cut him off from the system completely.

This calls for a policy requiring every path into the system to be controlled by the security software (RACF, ACF2, or TopSecret).

The standard paths into the system include: **batch jobs**, **started tasks**, **NJE** (Network Job Entry) and **RJE** (Remote Job Entry), plus **every applid**. Each applid, that is, each program with a signon screen, is a path into the system. This includes: **TSO**, **CICS**, **IMS**, and probably several dozen or more others. If **TCP/IP** is in use, then the TCP/IP daemons (like FTP) will be additional paths in. (These paths have been described in detail in earlier issues, and will be described further in future issues.)

To address this issue in your audit, you would look to see if there is a policy requiring all applids to call the security software to verify userids and passwords. You will want to know how well the policy is enforced. You might want to ask how management knows that there are no hard-coded lists of userids and passwords. Very likely they don't have a way of knowing unless they have had a formal review of all the applids.

Are Password Rules So Complex That They Weaken Security?

If you don't think about it too much, you might conclude that the longer the passwords are, and the more different types of character they have to contain, then the better the password strength. However there is a point beyond which increasing length and content requirements actually weakens the quality of passwords. When they become too cumbersome, then you can't blame people for writing them down, or for forgetting them.

This is especially true when users log onto several different systems on different types of computer, each with its own set of password rules.

Are Password Phrases and/or Mixed Case Allowed?

For a long time, the MVS operating system only allowed passwords with a maximum length of 8 characters. They were always upper case. The software vendors have enhanced the security software to support password phrases of from 9 to 100 characters. The security software now can support mixed case (upper and lower case) passwords and password phrases.

Some auditor may be tempted to insist on implementation of long password phrases and/or mixed case passwords. However, this is not practical until every program with a sign-on screen (every applid) is prepared to handle these.

What do Password Reset Patterns tell You?

If users have been trained in how to make passwords easy to remember, but difficult to guess, the number of password reset requests per week will be trivial. (Some specialists have estimated the total cost to an organization for a single password reset to be between $50 and $100.) Spikes in the number of reset requests may indicate an attack by someone trying over and over to guess passwords. What might you consider the significance to be if:

- The number of password reset requests was gradually increasing, so gradually that no one notices
- Management had no idea what the number of reset requests was, nor of whether it was rising, falling, or staying constant.
- The number of password resets was seemingly high. (What implications would this have for the quality of the security?)
- Password reset requests are not logged; password violations are listed one after another on the Violations Report, and no one plots reset requests over time.

How Can Log Data Reveal Passwords?

David Hayes of the GAO (Government Accountability Office) discovered this neat trick. During an audit, he looks at the SMF (log file) data for Monday morning logon attempts with invalid passwords. He finds that often after a pleasant weekend, users confuse their userids with their passwords. They enter their password where they

are supposed to put their userid. This reveals the password in the userid field of the log record.

David always knows that he still has to answer the "So what?" question. So he then reviews the dataset rules in the security software to see who has read access to the SMF data. This often leads to a meaningful audit finding and a practical recommendation on how to improve security.

So What's the Real Point About Passwords?

A deep security audit will evaluate how well passwords actually protect the system, and at what cost. This means determining how well management is aware of the number of password resets, the trend, and the price.

It also means evaluating how well users are trained or encouraged to make passwords that are "***easy to remember, but difficult to guess***".

When someone is surprised by the computer requiring him to change his password, he is likely to choose a new password based on whatever happens to be on his mind at the moment. This occurs while his mind is occupied with whatever work he is trying to accomplish. He is likely to specify a new password without focusing on it. This results in passwords that are both easy to guess and likely to be forgotten.

We have a different story if a user has a secret formula for devising new passwords, a formula that requires him to stop and think about the password. For example, he might use a formula that requires him to put the number 5 after the third character of whatever word he is using (**HOR5SE**, **BAS5KET**, **BAN5ANA**). If no one else knows his formula (there are a large number of such techniques possible), it will be difficult for a hacker to guess his password. The use of the formula, and the fact that he has to pause and focus to apply it, will make it more likely that he will remember his password.

So your audit can go beyond just checking password settings in the security software. You can review: whether all paths into the system are controlled by the security software; the number and trend of password resets, management's awareness of the number, and the training users receive on new passwords. From this, you can determine whether password protocols actually help improve the quality of security.

==========
==========

3) Questions to Ask at the PM (Post Mortem)

Smart project managers hold a post-mortem at the end of every major project, to discover what lessons can be learned. Here are some questions you might ask yourself and your colleagues after a major IS audit:

A. Did the audit make a difference?
B. What benefit does anyone think came from the audit?
C. Did we just follow a methodology, or did we also dig deeper to answer important questions?
D. Do the financial auditors understand what we did and how it affects their work?
E. Did we identify control objectives at the beginning of the audit and make sure every team member understood them?
F. What could we have done better?
G. What pleasant surprises did we encounter that we would like to repeat?

==========
==========

4) Free Sources of Great Information

CA's May Mainframe Madness:

Computer Associates is running a month long, free, Internet-based, opportunity to learn more about IS security and audit. Learn more at:

www.ca.com/us/content/campaign.aspx?cid=200004

Free Handouts:

Often speakers at user groups and professional organizations will put copies of their handouts on the Internet. Here are some examples of useful presentations available for free:

Handout for
"***RACF and Internal Control - Translating Effectively Between Both***" by Mickie Gray of GAO
www.stuhenderson.com/Handouts/NYRUG102009_InternalControl_b.pdf

Handout for Gwen Dente's Presentation "***Satisfying PCI Requirements with z/OS Communications Server and Selected z/OS Software Products***" on what you need to know if you accept payments by credit card
www.stuhenderson.com/Handouts/BWRUG_PCIStart_CS.pdf

==========
==========

5) Seminar Information and Miscellanea (Useful Articles, Proverb, Interesting Products)

5A) >>>>Seminar Information

Henderson Group seminars are available for in-house as well as public sessions.

The Henderson Group offers these "How to Audit..." courses :

- How to Audit **MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (May 4-7, 2010 in Raleigh, NC and November 16-19, 2010 in Clearwater, FL)
- How to Audit **z/OS with USS, TCP/IP, FTP, and the Internet** (April 6-8, 2011 in Bethesda, MD), a logical follow-on to the previous course

To learn more about them, please go to

http://www.stuhenderson.com/XAUDTTXT.HTM

5B) >>>>Useful Articles

How to Secure Mainframe FTP is described in an article at http://zjournal.tcipubs.com/issues/zJ.Dec-Jan08.pdf in the **zJournal**.

FISCAM (Federal Information System Controls Audit Manual) documents the approach to be used for IS audits of Federal agencies of the US government: www.gao.gov.new.items/d09232g.pdf

21 RACF Tips RACF is of course the security software for mainframe computers (it competes with ACF2 and TopSecret.) The handout from a recent ISACA presentation **"21 Things You Didn't Used to Know About RACF**" is available at:
www.stuhenderson.com/XARTSTXT.HTM

If you are involved in RACF audits, you should take a look. If you're involved in ACF2 or TopSecret audits, then you should look too, since the concepts apply (with different buzzwords) to those software tools as well.

Tape Security To learn more about why tape security requires special efforts, you might want to read this article titled "**Full Tape Security from Security Software and Tape Management Software**":
www.stuhenderson.com/TAPESEC1.PDF

5C) >>>>This Issue's Proverb of the Day

"*How do I make a beautiful statue from the block of stone? Simple, I just cut away everything that isn't a horse.*

How do I make a beautiful IS audit from all this data I could gather? Simple, I just cut away everything that doesn't relate directly to the financial control objectives."

5D) >>>>Interesting Products

While we generally do not recommend or overly criticize software products, we think you will find the following an interesting tool to consider to track changes to system software in z/OS systems:

- eventACTION and ussACTION among other functions provide an audit trail for z/OS Systems. For more info, contact Hugo Prittie at hugoprittie@actionsoftware.ch

(Please note that the "ch" in his email address is not China, but Switzerland, which is sometimes called the Confederation Helvetian. You can read all about the Helvetians in Caesar's "***Gallic Wars***".)

==========

.

About the Mainframe Audit News; How to Subscribe/Unsubscribe

The MA News is a free, email, newsletter for auditors who need (or suspect that they will need) to be auditing IBM mainframe systems (primarily MVS, z/OS, and the system software associated with them). This software includes: CICS, DB2, JES, VTAM, MQSeries, TSO, USS (UNIX System Services), TCP/IP, and others. It also includes the httpd daemon software which connects a mainframe to the Internet. (Note, we will expand each of these acronyms and explain how the software works over the course of past and future issues.)

The MA News is meant for auditors who are new to IBM mainframes, as well as for experienced MVS auditors who want to keep up to date with the latest developments from IBM. We will not make the list of subscribers available to anyone else for any reason.

To Subscribe, Unsubscribe, or Request Back Issues for the Mainframe Auditors' Newsletter (MA News)

Send an email to: **stu@stuhenderson.com** with the subject field set to: MA News and in the body of the email just the phrase you want: SUBSCRIBE or UNSUBSCRIBE or BACK ISSUES: 1, 2
