RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 78):

This Issue's Themes:

- Coming home to the Cloud
- Network Security
- Questions to Ask

Another Great Source of Free, Practical Info:

If you want to understand the security issues in Cloud Computing, you will want to read NIST's "***Guidelines on Security and Privacy in Public Cloud Computing***". This is their Draft Special Publication 800-144 at

http://csrc.nist.gov/publications/drafts/800-144/Draft-SP-800-144_cloud-computing.pdf

An Interesting Question to Ask Your Auditors:

"*What are the control objectives of the IS audit, and what are the control objectives of the financial audit*?" Even if you don't know or care what a control objective is, you will find the answers useful. For extra credit, ask how the IS control objectives support the financial control objectives.

New Website for the NYRUG: To simplify all the references, we have consolidated all info for the NYRUG and the Tampa Bay RUG at

www.nyrug.stuhenderson.com

NEW YORK RUG and Tampa RUG Meeting Dates

Tuesday, March 29, 2011 from 10AM to around 4PM. PLEASE NOTE THIS IS A SPECIAL MEETING WITH DIFFERENT TIMES AND REGISTRATION REQUIRED. THIS IS A LOT OF TRAINING AVAILABLE IN ONE DAY. **You will not be allowed to attend without pre-registering (it's free), as described inside.** Mark your calendars now. See inside for details and new website.,

(The meeting after that will be **November 1, 2011**)

NY Metro NaSPA Chapter (system programmers professional association) meets March 22, 2011.

You are warmly invited. Please RSVP and verify meeting details with Mark Nelson at markan@us.ibm.com

The meeting is open to non-NaSPA members and is free! Please pass this invitation on to your colleagues!

Vanguard Conference June 20-23, 2011

This great conference will be held June 20-23, 2011 in Las Vegas, NV. Learn more at:

www.go2vanguard.com/conference.php

Today's Quotation

"*Most of us fall somewhere on the spectrum between RACF clerk and Data Security Officer. It's the direction on that spectrum we're moving in that matters.*"

If Your Mainframe is Connected to the Internet and There's a Security Breach, Who's Considered Responsible?

You may not know whether your z/OS system is connected to your internal intranet or to the external Internet. Here are some of the ways the Internet could make it possible for a stranger in another country to access your mainframe data:

- telnet (remote logon)
- TN3270 (remote logon that acts like a 3270 terminal)
- FTP (File Transport Protocol, allows uploads and downloads of MVS datasets and USS files. Also handles submission of batch jobs and operator commands, access to printouts, and access to DB2)
- CICS
- DB2
- MQ Series
- Connect Direct
- NJE and RJE
- Others

This may seem daunting, but you should know that the z/OS system provides the most secure Internet connection (TCP/IP) of any computer around, if you properly implement the tools IBM gives us, including RACF. Here are some ways to ask yourself how secure your Intenet connection is:

- Issue the TSO command **NETSTAT** to find out what programs are talking over TCP/IP, and to what IP addresses. If there are none, then there may be no immediate risk.

- From the DSMON Class Descriptor Table Report, determine if the **SERVAUTH** resource class is active, and then list the rules defined in RACF for it. This is a powerful way to control use of IP addresses and ports.

- Does your organization have policy and standards regarding use of TCP/IP ports? Who administers the control files for programs that use TCP/IP? What change control and quality assurance do you have over the control files, the JCL, and the programs themselves? If some program decides to open a TCP/IP port, it can then read and write data over your TCP/IP network, subject to whatever controls you have in place. What authorization does it need? What controls do you have in place? (If someone wants to use a new High Level Qualifier for his dataset names, he needs authorization, and he needs to register the HLQ on some list, and to tell the RACF administrator about it. Shouldn't the same requirements apply to use of a TCP/IP port?)

- Do you know the name of your firewall administrator? Have you taken him to lunch?

Is the New z/196 Computer Just a "Cloud in a Box"?

IBM has just come out with a new version of the z series software and hardware. This one is called **z/Enterprise** and it executes on the new **z/196** hardware. We should not consider this just "another hardware upgrade with faster CPU and more memory". This has features which will constitute a revolution in how we configure our enterprise-wide (distributed and mainframe) systems. This will also introduce a new approach to cloud computing. And we will need to learn more buzzwords.

This will also introduce organizational change for enterprise-wide security administration. (Some may view this as a problem, others as an opportunity.)

Beyond impressive increases in CPU speed and memory, the z/196 provides a tight connection between the mainframe CPUs and an integrated blade server. A **blade server** is a stripped down collection of circuit boards which act as Windows or UNIX or other system servers. (Each server's circuit board (motherboard) is one **blade**. Imagine taking several UNIX and Windows servers from around your organization and putting them all into one box, getting rid of the unneeded keyboards, mice, monitors, and power supplies. That's a blade server.)

The **zBX**, zEnterprise BladeCenter Extension blade server which comes with the z/196 supports the LINUX, and AIX operating systems. It also includes an x86 processor which could conceivably run Windows or even VMware..

This blade server is tightly integrated by hardware and software with the z/196 mainframe CPU. It comes with the **z/Manager,** Unified Resource Manager to provide workload management and load balancing. The hardware connections provide tightly coupled data paths between the various operating systems, including MVS.

This means that we can replace the combination of a mainframe data center and several server farms with a z/196, supporting all the operating systems in the server farm. (We hope Windows will be added to the list soon, since the hardware is there to support it.)

The result will be faster data sharing, faster response time, greater flexibility to handle swings in workload, workload sharing, improved security and reliability, and lower costs. The overall cost for electricity and air conditioning will be lower too. And it can all connect easily and securely to the Internet.

This seems to give us all the advantages of cloud computing, without having to transport our sensitive data out of our control to some other company that needs to make a profit off what they charge us.

Who administers information security on your distributed platforms now? Do you expect this to change if all the distributed servers are consolidated into one blade server in the data center, tightly coupled to the z/OS CPUs? Is your organization encouraged to cut costs by consolidating duplicate staff? And is it easier for a RACF administrator to learn LINUX or for a LINUX administrator to learn RACF?

Wouldn't it be interesting to know Microsoft's take on all this? (Remember when IBM and Microsoft worked jointly on what became Windows and OS/2?)

Interesting Products

While we generally do not recommend or overly criticize software products, we think you will find the following new products of interest:

ESSF, the EKC Security Services Facility, is a new program product to provide enhanced functions for IBM z/OS Resident Security Systems ("RSS"), including RACF..

- Automatically archives profiles as changes are made to the RACF Database(s)
- Password changes by a user may be automatically propagated, even when actual userids are different.
- Instantaneous profile recovery into the active RACF system environment from the ESSF archives at any time.
- Clones Users along with all corresponding accesses, connections, and user dataset profiles.
- Displays, copies Group or User access, connections, and/or profiles.
- Repairs damaged RACF databases.
- Cleans up dormant profiles

Contact Sales@ekcinc.com for more information on EKC Software Products.

==========

Vulnerability Assessment Tool

At the last meeting of the NYRUG, we described a dedicated Systems Programmer who wrote programs which automatically looked for security flaws in privileged programs by calling them with a variety of different inputs. The result of this work is the **Vulnerability Analysis Tool** from Key Resources, Inc. and it is now available on either a license basis or as part of a system integrity vulnerability assessment. For more information, go to www.vatsecurity.com. (I wonder if I buy it in Europe, is there a VAT on VAT?)

==========

ZEN System Event Monitor

captures, views, filters, notifies SyslogD events in real-time, including security violations. Provides triggers for powerful REXX-based automation facilities.

Contact: Graham Storey, William Data Systems, (703) 674 2200,
graham.storey@willdata.com, www.willdata.com

==========

Voltage SecureData Encryption Technology

adds controlled encryption technology to existing applications for regulatory compliance, and without key management headaches. Uses the AES Encryption algorithm in an advanced mode known as "Format-Preserving Encryption" (FPE). FPE allows you to encrypt things like credit card numbers or addresses, and the encrypted versions match the format of the originals (n decimal digits, etc.), thus avoiding the need to redo database schema, screens, and the like. Product is multi-platform, with multiple levels of encryption.

Contact: Phil Smith III, phil@voltage.com, www.voltage.com, (703) 476-4511

Is SNA Dead?

SNA (IBM's System Network Architecture) has been rumored to be dying, much like the mainframe. And both sets of rumors are mistaken! Here's why some people think that TCP/IP is eliminating SNA from the world, and what they are missing, and what it means for network security:

1. When you log onto TSO from a terminal, the terminal is now connected to the mainframe by TCP/IP (it used to be an SNA link.)

   The Real Story: *Your terminal is still using SNA, but the SNA is tunneled inside TCP/P*.

2. When we connect our mainframe network to our business partner's mainframe network (maybe we're a bank, and they're a credit card processor, for example.), we've replaced SNA with UDP/IP (**UDP** is a protocol, sort of like TCP.). We're using **EE** (Enterprise Extender) to do this, which is IBM's recommendation.

   The Real Story *You haven't replaced SNA, you are merely tunneling it through UDP, which is a protocol sort of like TCP.*

So why should I, a RACF security administrator and Data Security Officer care? Some people think we don't need to address SNA security, in the belief that SNA isn't there any more. It is there, and using encryption and firewalls to protect the TCP/IP and UDP/IP envelopes around it won't protect against SNA security exposures.

In particular, if your SNA network is connected to a business partner's SNA network (likely using Enterprise Extender), you may be exposed to some risks very similar to TCP/IP risks (man-in-the-middle attacks, Denial of Service, Password Harvesting). To learn more about this, and to see examples of case studies and actual attacks, you might take a look at www.net-q.com.

These risks are the result of a change in design attitude for part of **VTAM** (IBM's Virtual Telecommunicaton Access Method, the software that manages all terminal and telecommunications connections to the mainframe, including TCP/IP and UDP.).

From VTAM's start, it has almost always allowed connections only when everything (every terminal, every piece of software, every program involved) had been defined to VTAM in advance. This is in contrast to the open approach taken by TCP/IP.

When you connect two companies' SNA networks though, the volume of things to manage grows dramatically. So VTAM's developers took a more open approach for the part of VTAM that handles this (**APPN** for Advanced Peer to Peer Networking).

Because of this more open approach, things don't need to be pre-defined to VTAM. This provides greater flexibility. It also increases the need to authenticate (prove the identity of) all the partners. If your company's network uses EE with APPN to talk to another company's network, you may be exposed to the other networks that that company is connected to, and to the networks they are sharing with and so on.

This can lead to the risk of a program in one of these other networks spoofing (stealing the identity of) your or your partner's networks and VTAMs. The risk is manageable, but only if you evaluate it and take reasonable precautions. IBM gives us some tools to mitigate the risk, including VTAM start-up options, network configuration options, the **APPCLU** and **VTAMAPPL** resource classes in RACF, and others.

Do You Have the Information You Need to Do Your Job?

Suppose that you are a RACF administrator / Data Security Officer. You need to answer several questions:

- What laws and regulations apply to the data you are supposed to be protecting and which specific datasets do they apply to?
- What are the pros and cons of encryption, Erase-On-Scratch, and other ways of protecting residual data?
- Which datasets have sensitive data and therefore need to be protected as residual data, both on tape and on disk?
- What should you be doing to protect USS (Unix System Services)?
- What should you be doing to protect mainframe TCP/IP?
- Which resource classes should you be using and how?

The problem with many of these questions is that you don't have the answers; someone else does. What are your auditors doing to help you get the answers? What is your manager doing? What are you doing?

NYRUG (New York RACF Users Group) and Tampa, FL RUG March 29, 2011 from about 10AM to 4PM:

Our next meeting is at DTCC in downtown Manhattan. This is a joint meeting by teleconference with the Tampa FL RUG. Attendees **must present a government issued photo ID** to enter the building. Admission is free, but even if you have registered for previous meetings, you must pre-register by emailing NO LATER THAN NOON the day before. Please see the new website listed below to register.

Please note that speakers no longer provide copies of handouts. You can print your own copies from the new website listed below.. Our exact agenda is not certain at press time, so you might want to check the same site for exact details as they become final.

The Fall Meeting will be November 1, 2011, also at DTCC. We bet you know where to find the details as they become available.

For Complete Directions and to Register, Please Visit the New Website for the NYRUG and TBRUG: at www.nyrug.stuhenderson.com

This website has

- Directions to both meetings
- Easy registration links
- Current version of the Agenda (subject to change)
- Links to get copies of handouts

HG RACF Training Schedule:

The Henderson Group offers its RACF and computer security/audit seminars around the country and on-site too. See the details below or call (301) 229-7187 for a free seminar catalog. For more info or to see what students say about these classes, please go to **www.stuhenderson.com**. (See info on "Mainframe Audit ..." classes below.) You can save money by holding a class session in-house, or by hosting a public session. Contact Stu for more info.

1) HG04 **Effective RACF Administration** (**$1995**)
Mar. 1-4, 2011 in Clearwater, FL
Dec. 5-8, 2011 in Bethesda, MD

2) HG05 **Advanced RACF Administration ($2050)**
May 23-26, 2011 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
April 11, 2011 in Bethesda, MD

HG Mainframe Audit Training Schedule:

The Henderson Group now offers its series of "How to Audit.." seminars for IT auditors. These describe clearly how the associated software works, where the control points are, how to collect and interpret data, and how to conduct the audit. The workbooks include complete audit programs. More information is available at our website: **www.stuhenderson.com** (If you have a class topic you would like to have added to this series, please let us know. (See info on "RACF Training" classes above.)

A) HG64 **How to Audit MVS, RACF, ACF2, CICS, and DB2** (**$2100**)
May 9-12, 2011 in Raleigh, NC
Nov. 7-10, 2011 in Clearwater, FL

B) HG65 **How to Audit z/OS with USS, TCP/IP, FTP, and the Internet**
(This class is a logical follow on to HG64.) ($1590)
April 6-8, 2011 in Bethesda, MD

.**Permanently Interesting Products Column**

This column has been permanently moved from this newsletter to Stu's website. You can find it at:
www.stuhenderson.com/XINFOTXT.

RACF User Services (Newsletter Subscriptions / Key Phone Numbers / Addresses)

Technical support hotline, Meetings, Free Newsletter subscription, Seminar Catalogs:
Stu Henderson - (301) 229-7187
5702 Newington Rd, Bethesda, MD 20816

For Back Issues of this Newsletter and Links to Several Useful Web Sites

check the Henderson Group website at:
www.stuhenderson.com

RACF List Server on the Internet

To join, send E-mail to the administrator for the server. (Don't send it to the server itself or your request will be routed to every subscriber.) For example, if your name is John Smith and you want to subscribe, then send this E-mail:

subscribe racf-l john smith

to the address: **listserv@listserv.uga.edu**

The reply will include directions on how to get info such as a list of all subscribers, an index to previous comments, and a command summary. You will want to set up a filter for incoming emails to direct mail from the list server to a dedicated folder or directory.

Free Email Newsletter for Mainframe Auditors

To learn more about the Mainframe Audit News (MA News), check Stu's website:**www.stuhenderson.com** .

To Get a Free Subscription to the RACF User News Phone Stu at (301) 229-7187 with your request, leaving your name, postal address (sorry, only US postal addresses; others will need to read issues online), and phone. For back issues and articles on topics like the **SERVAUTH** resource class, check his website: **www.stuhenderson.com**

The RACF User News is published two or three times a year to share information about RACF. All information in it is offered on an "as is" basis, and should be used at your own risk, and with your own testing.

Other Internet places:

- RACF Password Cracker Program. Email Peter Goldis at **pete@goldisconsulting.com** or look at **www.goldisconsulting.com**
- Georgia RUG at www.garug.net ..
- Thierry Falissard's RACF page is **www.os390-mvs.freesurf.fr/**
- Nigel Pentland's security page is www.nigelpentland.co.uk
- IBM RACF home page: www.ibm.com/servers/eserver/zseries/racf/
- RACF goodies site: www.ibm.com/servers/eserver/zseries/zos/racf/goodies.html
- RACF Presentations Page with lots of presentations from SHARE and GSE. Check out http://www.ibm.com/systems/z/os/zos/features/racf/presentations.html
- IBM Redbooks site: www.ibm.com/redbooks
- IBM z/OS Manuals: www.ibm.com/servers/eserver/zseries/zos/bkserv/
- Net-Q SNA Security case studies and examples at www.net-q.com.
- (Other vendors contact info listed in the "Permanently Interesting Products" column which is now moved to Stu's website at:**www.stuhenderson.com/XINFOTXT.HTM**
- the Henderson Group: **www.stuhenderson.com**

21 Things RACF Auditors Should Know:
This PDF file lists 21 things for auditors, including a reference on why you don't need to protect the program AMASPZAP with RACF. The article is available at:

www.stuhenderson.com/XARTSTXT.HTM

More Info on Tape Security and RACF is available in the following article from the zJournal:

http://www.zjournal.com/index.cfm?section=article&aid=762