Global Information Assurance Certification Paper

Using a Combination of Microsoft Access and TASA (The Automated Security Attendant) to Identify and Remove Unused User Ids from RACF

By Jaime Cartagena submitted October 19, 2004
For GSEC Certification

In this practical assignment I will discuss how I used existing tools to identify and remove unused user ids from a RACF security database that defines access control to an online CICS Policy database. It will outline the different steps and processes performed in order to accurately identify and report in addition to removing these ids from the database. It will detail how I used a Microsoft Access application created specifically for reporting on a RACF database and TASA (The Automated Security Attendant) to achieve the final goal of removing Information Security vulnerability and put us more in line with standard security practices. Using this process, I identified and removed 973 unused ids of which 672 were unrevoked! It really brought home the fact that we cannot take security for granted and that we must audit our security databases regularly to identify potential risks to the system. It also made me appreciate the inherit power and flexibility of Microsoft Access and how it can be an exception tool for reporting on all types of security databases.

Everyone knows that having old unused ids on your system is an Information Security issue. In addition to creating more overhead for the system, it also shows up on those Security Audits that we have to submit to. The following is an excerpt from the SANS website itself on the Twenty Most Critical Internet Security Vulnerabilities – The Expert Consensus paper posted on the following SANS website:
http://www.sans.org/top20/index1.php/hacktech_wt04/hipaa_boston04 states:

> Validate the list on a regular basis to make sure no new accounts have been added and that unused accounts have been removed.
>
> Have rigid procedures for removing accounts when employees or contractors leave or when the accounts are no longer required.

Being a member of the newly formed Privacy and Information Protection Services Department, my job is to get the RACF security database I inherited from a previous department cleaned up and in shape. As part of our project on minimizing our security vulnerabilities, we have scoped out several items that we wanted to address as our top security issues that needed to be resolved. One of those items that appeared on an independent Security Review was our process for removing user accounts from our database which were not being used or belonged to anyone currently in the company was considered poor. They consisted of ids that were both in revoked and unrevoked status. Due to several years of poor administration and policy, the procedure for removing users after they have left the company was to simply revoke the id and not remove it. The "mode" of thinking was that if the employee ever returned to the company, they only needed to resume the id and the user could resume work as if he/she had never left the company. This procedure goes against the guidelines based on id and password standards and best practices listed in the state of North Carolina Information Resource Management Commission's Information Protection Policy found on the following website:

http://irmc.state.nc.us/documents/approvals/id_authentication.pdf It says "Promptly remove a user id, when the user is no longer employed by the agency or no longer requires access to the information system."

So as one of our quick hits to the database, our company's Information Security Officer gave me the task of identifying all the unused ids and removing them from the RACF security database. I then came up with the criteria to be used to identify these unused accounts. These accounts according to an excerpt of the July 2000 issue of Computerworld posted below on Waveset's website http://www.waveset.com/Features/inside_threat.html strongly suggests that unused user ids is a big problem with large corporations.

"Some 30% to 60% of the access profiles in large corporations are no longer valid, according to Chris Christiansen, a security analyst at IDC. In Framingham, Mass. **Unused user IDs, passwords and remote access permissions are a magnet for even amateur hackers,** he said."
Old IDs Never Die; They Just Cause Trouble
Computerworld, 7/31/2000

These unused accounts that would possibly have varying degrees of authority to confidential and private information could be used by a hacker or insider to gain access to restricted information or even worse tamper with it. This was a risk that we considered unacceptable and needed to be quickly addressed. So I created the following criteria in order to identify these accounts. Remove all ids that have not been used for more than one hundred twenty days that are either in revoked or unrevoked status and that do not belong to current employees of the company. Simple enough you think? Sure, but to create the reports you want to backup your work using the limited reporting capabilities of RACF is not an easy task in itself to undertake. But with a little ingenuity and tools that we currently have in place at the worksite, this task can be done. Below describes how I identified and removed these ids from our RACF security database and closed a gaping hole in our Information Security program.

First, our company under direction of the Information Privacy and Security Officer purchased a tool that at the beginning of this year called TASA (The Automated Security Administrator). This product created and sold by InfoSec Inc. can be found on the following website: http://www.infosecinc.com/products/TASA.htm . This is an excellent tool of which I highly recommend for every RACF Security Administrator out there. One of the main uses of this tool is to monitor activity to a RACF database and identify what resources are not being used by any particular id that has access to it. For example if a user is transferred to a new department but the person's previous access was never removed and not used in the new department, TASA will identify that unneeded resource and even code the commands to remove the user's access, and recreate the id if need be. It is of immense help in identifying unused resources defined in a RACF security database as this type of information is very difficult to identify easily. Below is a

small excerpt from TASA's website describing the background reasoning for the creation of this product.

Inactive user IDs are difficult to identify and remove because user ID "last use" dates provided by the security system are not always reliable. These dates are not maintained for Automatic Terminal Sign-on (ATS), Network Job Entry (NJE), JES Multi-access spool (MAS), and others. Unknowingly, user ID cleanup based on "last use" dates has often caused serious problems when vital production user ids were inadvertently judged unused and deleted. As a result, inactive user ids are most often left to accumulate.

Secondly, the company had an independent consultant by the name of Robert F. Kennedy come in and help us with some separate RACF training issues we had. He also created a Microsoft Access based application of which I call the RACF Reporting Tool. It simplifies and extends the reporting capability that we had previously RACF. It is extremely useful when it comes to creating custom reports for security audits that cannot be easily created using the native reporting capabilities in RACF. Basically what this application does it take a copy of the unloaded RACF database and loads it into a Microsoft Access Database for reporting. This application has many canned reports built into it and one of those is an unused user report listing. If anything, I highly recommend hiring him as a consultant and having him install and train you on the use of this application. It will save you time and money in the long run. Not to mention the ease of administration that it provides.

In this project, I used RACF Reporter to identify the ids that I wanted to delete and then used TASA to both confirm my deletions and create the commands to both perform the deletion and recreate the id if need be. Using this process, I identified and removed 973 unused ids of which 672 were unrevoked! To put this more in perspective, our company has a total of 1051 employees. This definitely puts us in line with the statement made by Chris Christiansen quoted above four years after it was made. To say in the least, I was very surprised by the large number of unused ids and the gaping security hole that it represented! Imagine a hacker given the chance to crack the passwords 672 unused ids that are not being monitored. He or she would definitely have an advantage over another hacker who did not have that amount of ids available to crack. In this paper, I will not mention the name of the company and have sanitized the data for security purposes.

Now as stated before, I wanted to remove all ids that have not been used for more than one hundred twenty days that were either in revoked or unrevoked status and that do not belong to current employees of the company. Well using the RACF Reporter application written by Robert Kennedy, which unloads the RACF security database using the IRRDBU00 unload utility and then loads that data into the Microsoft Access database, reporting is much easier and more powerful. You can create all sorts of reports to analyze your database. One of

the reports that Robert created is ids that have not been used in 120 days. Now pulling that information into a separate Access table and matching the Employee Master File that we have both on id and then on name to separate those id's that belong to active employees of the company. Using this technique, we were able to identify 973 total unused ids that did not belong to any current employee of the company.

The key file that we had here is the Employee Master file from Human Resources. In the Security realm, it pays to investigate files that might exist on your system which can simplify your life. There is no need to reinvent the wheel if the data that you are looking for already exists and is being maintained somewhere else in the company. It took one simple meeting with the Human Resources department to discover that had exactly the file that we were looking for. Not only did it have the name information of course, but also their assigned id. This worked great and saved us a huge amount of work trying to accumulate this information ourselves. Again, I stress it pays to put yourself out there in your company and to talk to other departments.

One kink that we encountered is that our users may have multiple ids defined on the RACF database. There have been several acquisitions by our parent company over the years. Those acquisitions had CICS applications which were ported over to our mainframe. In order to simplify the porting, the ids that existed on that application were ported over as well. In addition, these users had new user ids created on our system as part of the integration. Because of this a user might have a maximum of four separate ids on the same system. As one of the parts of initially installing the Microsoft Access application was to make sure that the multiple ids had exactly the same name defined to each of them so and that it also matched our HR Employee Master file exactly. That way we could match on name if we needed to in order to find all ids that a user was associated with.

Now with that said and done I was able to identify the ids that needed to be deleted. First I will describe to you the process in a brief summary and then detail it in the next pages so that you can use this process at your location to do the same.

Step 1 - Load all ids from RACF into Microsoft Access Database for reporting.
Step 2 – Run the canned report to list all ids that have been used for more than one hundred twenty days. Remove any system ids or any special ids. We in some instances have ids that need to be defined but are in revoked status. Load that data into a separate Microsoft Access table.
Step 3 - Load HR Employee Master File in Microsoft Access table.
Step 4 - Match the unused id table created in step 2 to Employee Master File created in step 3 both on id, then name. Flag any matches on the unused table.
Step 5 - Take user ids left from step 5 and run them against the TASA (The Automated Security Attendant) to create two files. One is the

command file to delete the ids; the other is a command file to recreate the ids if an id was accidentally deleted by mistake.

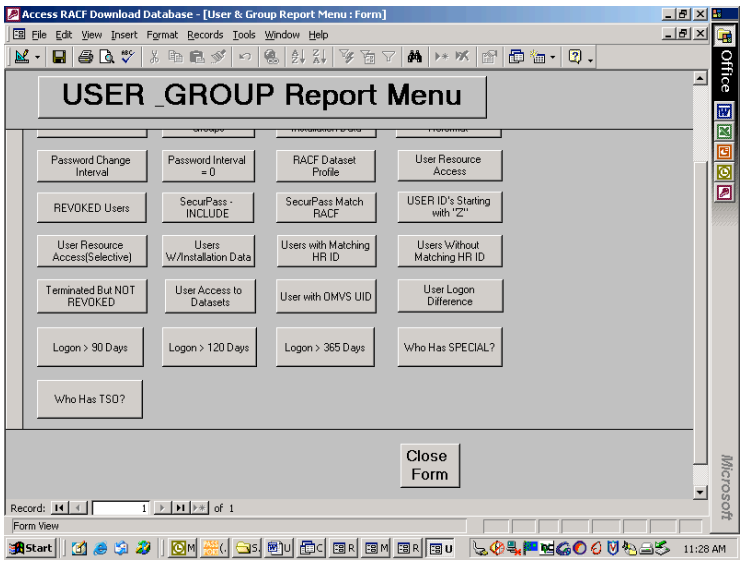
Step 6 - Wrap JCL around the delete command file and run against RACF to remove the unwanted ids.

This in a nutshell describes the process that I used to identify and remove the ids that my Information Security Officer wanted identified and deleted with the least amount of work and the most amount of accuracy as possible. As you might be able to tell from above, I used to be a programmer and therefore take a task and break it down into its simplest of components. Now below, is detailed how each step was actually performed.

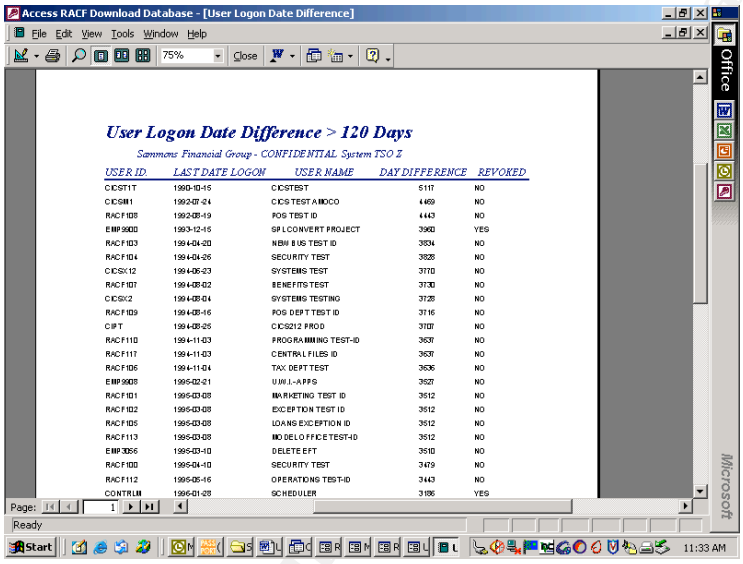
Step 1 - Load RACF Database into Microsoft Access Application (RACF Reporter)

This step is simple as the application has modules built to do this at the click of a mouse. It is a four step process. First you must run the RACF unload utility IRRDBU00 to create a complete unload of the RACF database. Next you ftp that mainframe file over to the load directories that RACF Reporter uses to refresh its tables. Then you bring up the RACF Reporter application and first click on the button to clear the existing data from the tables. Then you click on the button to reload the data into the tables. This will give you a current snapshot of how your RACF database looks.

Step 2 - Go over to the reporting section of RACF Reporter and run the canned report “Logon > 120 days” shown below and export it to a Microsoft Excel format for processing by clicking on the export option on the File drop down menu. Once in Excel, I create another worksheet and paste the information onto it so that I can keep a “before” view of the data. To do this, you select Insert worksheet from the insert command on the toolbar. Then in this new worksheet, I then sort the data by name and id. Sorting it like this allows me to identify if a user has more than one user id defined to the system. I then create a new column into which I merge the last and first name fields together so that the format matches the name on the RACF database. This format will match the name format on the Employee Master file. It also makes for easier matching on name in a later step. I then go in and manually remove any system ids and special ids. This is fortunately easy as the company I work for uses a naming convention for our ids. All ids the begin with EMP0 and EMP9 are special ids (Id’s that are used some time for non-routine processing which are resumed when they need to be used and revoked when they are not being used).



Report menu on RACF Reporter Application



Sample Logon > 120 Days report generated from RACF Reporter

Then, I cut all the reformatted records and past them into a new Notepad document and save that files as “Ids not used_120 days.txt. I create a new table in Access called “Unused ids” and load the text file into it. This table for simplicity sake contains the ID, Name (Last, First), and Employee flag field to identify if the id belongs to a current employee of the company. This table will be used in later steps for further processing. Creating tables in Microsoft Access is also a simple task as it allows you to create it easily using the wizard or in design view. I create the ID field with a length of seven characters and the name field for a length of twenty five characters. Twenty five characters is the size of the name field in RACF. The employee flag is created with a length of three characters so that I can set it to “YES” if I find that the unused id belongs to a current employee of the company.

Step 3 - Load the Human Resource Employee Master File. For simplicity sake I only load the data that I need from the file. That information is ID and Name. I basically perform the same step as I did in step 2. This file is in a comma separated format which I save and process in Excel. After processing, I then paste the information into a Notepad document and save it as a text file. Using Excel, I reformat the id information into uppercase (it is not necessary as Access will match upper against lowercase letters, but I like organization and order so therefore I do it.) Then I merge the last name and first name fields together as in step 1 so that the format matches that of the RACF database. This is done by entering the following formula in Excel: fielda&","&fieldb. Saving that information in Notepad, I then create a table called "Employee Master File" containing the following fields, id and name. The id field will be seven characters long and the name will be twenty five characters long. This table will then be matched against the unused ids table to flag ids that belong to existing employees. Again, using Microsoft Access is easy as someone with my limited experience was able to create tables, queries and reports in little time by using the wizards and menus built into it. My experience with Microsoft Access was absolutely none prior to this project and within days I felt very comfortable using this product and maneuvering through the different menus. I recommend to all Security Administrators that they take the time to learn Access and its features as it an extremely powerful yet simple tool that can be used in many ways to simplify day to day processes that many of us administrators must do at our respective companies.

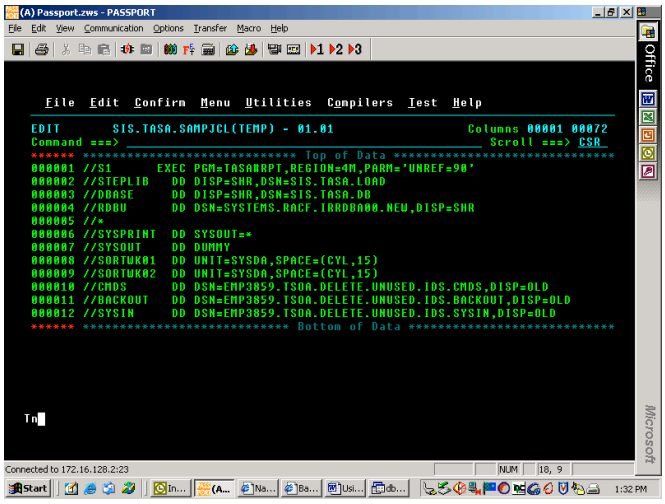
Step 4 – Match the unused id table to the Employee Master table both on id and then name and flag those matches by updating the employee field on the unused id table to a "YES". Again Microsoft Access allows you to easily do this in design view by dragging and clicking on a few items. As an example below I was able to create an update query by first selecting the query type in design mode, then selecting the tables I wanted to use by double clicking on their names and finally setting a value of "YES" to the employee flag on the Unused id table. I created two update queries, one which matched on id, the second which matched on name. Using this process, I matched a total of one hundred ten ids to existing users. Our company has several users that only use their mainframe account only once a year so which is why I found these unused ids matching to current employees. Much of what they do pertains to budgeting for the next year and year end closing.

Step 5 - Finally create a report in Access to select all record in the Unused ID table which does not have the employee flag set to "YES". This will select all ids which does not belong to a current employee of the company that you want to remove from the system. Select only the id field to display on the report. The following step only requires the id to be used as input. Export the report into a text format by selecting the export option on the file drop down menu and save it as a text document "Nonemployee unused ids.txt".

Step 6 – FTP the “Nonemployee unused ids.txt” to the mainframe for processing by the TASA software agent. TASA once set up is a powerful tool for administrators using RACF, ACF2 or Top Secret security databases. What I like to do is to load all resources into TASA for monitoring as it does not affect system performance and gathers information over time on the resources used in a security database. I use the all command shown below to load all security profiles such as data, group, and resource profiles into the TASA agent for monitoring. One great feature of TASA is that it will generate the commands for you to delete and recreate a particular resource. As I indicated in this paper that a total of nine hundred seventy three ids were identified as an unused id that did not belong to a current employee of the company and which had not been used for a minimum of one hundred twenty days. To manually delete or create the batch commands to delete them would be cumbersome and prone to error. One would need to investigate what resources a particular id had access to and remove that access and finally remove the id from the RACF database. Ids which are set up for use in TSO requires additional steps to remove the dataset profile that is created for them and the alias that removes them from the catalog. TASA takes care of all of this cumbersome work by creating the batch commands to do all of this. Not only that, it will create a separate file which contains the batch commands for recreating in my case any id that I may have mistakenly removed and will recreate that id and all the access it had prior to its deletion. It is an excellent tool which no RACF, ACF2 or Top Secret Security Administrator should not be without.

To create the command and back out command files using TASA, I use JCL to call on TASA’s report generator. On the input sysin statement, I point to the file that I FTP’d from Microsoft Access to the mainframe called “Nonemployee unused ids.txt”. On the parameter segment I indicate to TASA that I want non-referenced resources for a period of time. In my case, TASA was up and running for ninety days collecting information. The longer TASA is running the more information it gathers on resource usage. For example a resource might not be used for five months. If TASA is left running for that period of time, then it will identify that resource as not being used for five months. The ninety days it was running collecting information I felt was adequate to confirm that the ids that I identified to be deleted were in fact not being used and could be deleted without creating any detrimental effect.

Running the JCL called RPTTASA below, I created two files which were called EMP3859.TSOA.DELETED.UNUSED.COMMANDS which are the batch commands to delete the ids that TASA has confirmed as not being used and EMP3859.TSOA.DELETED.UNUSED.BACKOUT to create the commands to recreate any ids and accesses if need be.



I referenced the first file in my RACF JCL which calls IKJEFT01 to process batch commands in RACF and ran it to delete the unused ids during a Tuesday morning. One thing I learned from my manager is never to run any type of job which updates RACF in a significant way as this on a Monday morning or Friday night unless I wanted to affect a Monday morning process or work the weekend trying to fix possible problems. Deleting the ids on Tuesday morning allowed me to avoid the Monday process and ensured that I would be in the office if anything went wrong. Fortunately in my case, nothing did go wrong and it has been several days since the project was completed with no calls or notifications from other departments saying that are missing ids.

Working on this project has helped me in many ways. Not only has it allowed me to learn how to use Microsoft Access and TASA, but has also opened my eyes on the importance of making sure that unused ids are removed as it leaves one less vulnerability on someone gaining unauthorized access to our system. Be it either from the inside or outside. According to research and the SANS Security Essentials course which I took, most attacks come from the inside by the company's own employees. If an employee knew of any ids that I identified in this process, and was able to crack its password, access to privileged information might have been gained and the damage to the company in terms of its image and integrity might have been very large. Not to mention possibilities of legal ramifications as we store data that fall under the directives of HIPAA. We also maintain credit card, bank information and other personal information on tens of thousands of people located throughout the United States who carry insurance policies with our company. This information can fall under the jurisdiction of different laws such as California's SB 1386(Peace)/AB 700 Simitian which requires us to disclose to any California resident on our file of a security breach if we reasonably believe that it was compromised by unauthorized user. This law can be found in detail on California's Privacy Protection website: http://www.privacyprotection.ca.gov/leg2002.htm.

It has also allowed not only me, but also my company's Information Security Officer to feel better about the state of our Information Security. She feels more confident that we are not overlooking the simple things that we can do in order to better protect a company's assets. She also feels that this "quick hit" to the RACF security database closes an obvious vulnerability, which could have been used to compromise our information security.

References

---. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus.” 8 Oct. 2004 URL: http://www.sans.org/top20/index1.php/hacktech_wt04/hipaa_boston04 (8 Oct. 2004)

North Carolina Information Resource Management Commission’s Information Protection Policy URL: http://irmc.state.nc.us/documents/approvals/id_authentication.pdf (9 Oct. 2004)

Cope, James, ”Old Ids Never Die; They Just Cause Trouble.” Computerworld. 31 July 2000 URL: http://www.waveset.com/Features/inside_threat.html (9 Oct. 2004)

TASA (The Automated Security Administrator). URL: http://www.infosecinc.com/products/TASA.htm (8 Oct. 2004)

1386(Peace)/AB 700 (Simitian) of 2002 – Notice of Security Breach. California Department of Consumer Affairs Office of Privacy Protection. URL: http://www.privacyprotection.ca.gov/leg2002.htm (6 Oct. 2004)