SF-SECUCLEAN®

SECURELY IDENTIFY AND ELIMINATE REDUNDANT PROFILES AND EXCESSIVE AUTHORIZATIONS IN RACF

YOUR GOALS

EFFICIENT LONG-TERM MONITORING OF ALL ACCESS REQUESTS TO Z/OS RESOURCES

RISK-FREE REDUCTION OF AUTHORIZATIONS DOWN TO A "NEED TO HAVE" BASIS

SAFE DELETION OF PROFILES

CLEAN UP THE RACF DATABASE AND OBTAIN AN INITIAL ROLE MODEL

AN ELEMENTARY FACT REGARDING SECURITY BECOMES VERY APPARENT WHENEVER YOU REACT TO THE RESULTS OF A **Z/OS PENETRATION TEST OR AUDIT,** AS WELL AS DURING THE **INITIAL SETUP OF A ROLE MODEL:** IT IS PARTICULARLY DIFFICULT TO ELIMINATE EXCESSIVE OR REDUNDANT AUTHORIZATIONS IN RACF, I.E. TO STREAMLINE ACCESS LISTS, LOWER THE UNIVERSAL ACCESS AUTHORITY (UACC) OR EVEN DELETE PROFILES. CLEANING UP THE RACF DATABASE AND THE SUBSEQUENT "TIGHTENING" OF YOUR EXISTING SECURITY CONFIGURATION IS SIMPLY ONE OF THE MOST "FEARED" CONSEQUENCES OF ANY AUDIT REPORT OR ROLE-MODELING PROJECT.

WHAT ARE THE PRACTICAL PROBLEMS INVOLVED WHEN CLEANING UP THE RACF DATABASE? TO RETROACTIVELY IMPROVE A SYSTEM'S SECURITY, I.E. TO QUESTION EXISTING AUTHORIZATIONS BY REMOVING, REORGANIZING OR REDUCING THESE, ALWAYS INVOLVES THE REAL RISK OF NEGATIVELY INFLUENCING PRODUCTIVE PROCESSES AND PROVOKING SUBTLE FAILURES. ACTUALLY, A GOLDEN RULE IN IT IS TO "NEVER CHANGE A RUNNING SYSTEM!" NOBODY KNOWS WHICH USERS ACCESS WHICH RESOURCES AND WOULD EVENTUALLY SIGN A CORRESPONDING STATEMENT AS DEFINITIVE. MANAGEMENT IS THEREFORE CONSTANTLY CHALLENGED TO PROVIDE THEIR SECURITY TEAM WITH THE NECESSARY MOTIVATION FOR SUCH A CLEANUP PROJECT WHILE TAKING INTO ACCOUNT ITS PRIMARILY ABSTRACT VALUES OF SECURITY AND COMPLIANCE. AT FIRST GLANCE, IT SEEMS AS IF EVERYONE INVOLVED "HAS NOTHING TO GAIN." BUT THIS IS NO LONGER TRUE – THERE IS GOOD NEWS!

THE RIGHT TECHNOLOGY AND SUPPORT MAKE IT EASY TO CLEAN UP RACF – AND ALSO WORTHWHILE FROM A PRACTICAL POINT OF VIEW. DELETED PROFILES, STREAMLINED ACCESS LISTS, COMPACT GROUPS – ALL THESE AVOID OVERHEAD IN RACF'S PROCESSING AND THUS SAVE CPU TIME CONCERNING EACH RESOURCE ACCESS CHECK – SEVERAL MILLIONS OF WHICH OCCUR DAILY.

SETTING UP AN INITIAL ROLE MODEL CREATES CHALLENGES QUITE SIMILAR TO A RACF CLEANUP. THE FIRST STEP IS TO DEFINE THE CURRENT STATUS QUO OF THE REQUIRED AUTHORIZATIONS FOR ALL USERS. YOU MUST DETERMINE WHICH RESOURCES EACH USER MUST ACCESS REGARDING HIS OR HER "ROLE(S)" IN THE COMPANY'S BUSINESS. A COMPLETE AND COMPREHENSIVE ASSESSMENT IN THIS FIELD IS A PREREQUISITE FOR THE SECOND STEP, WHICH INCLUDES THE DEVELOPMENT OF A ROLE MODEL BASED ON EFFECTIVELY REQUIRED, I.E. NON-EXCESSIVE AUTHORIZATIONS.

BOTH CHALLENGES – CLEANING UP RACF AND SETTING UP AN INITIAL ROLE MODEL – PROVOKE A COMMON TECHNOLOGICAL DESIRE TO PERFORM A LONG-TERM OBSERVATION OF ALL RESOURCE ACCESS REQUESTS. SF-SECUCLEAN PROVIDES YOU WITH THIS EFFICIENT LONG-TERM MONITORING FOR RACF ENVIRONMENTS. ITS HIGH PERFORMANCE AND COST-EFFECTIVE TECHNOLOGY ALLOWS YOU TO EASILY 1) CLEAN UP AND STREAMLINE THE SECURITY CONFIGURATIONS DEFINED BY THE RACF DATABASE (E.G. STREAMLINING ACCESS LISTS, LOWERING UACCS, REMOVING GLOBAL ACCESS AUTHORIZATIONS, DELETING PROFILES, ETC.), AND 2) PERFORM THE NECESSARY ASSESSMENT OF THE CURRENTLY REQUIRED ACCESS AUTHORITIES TO SET UP AN INITIAL ROLE MODEL.

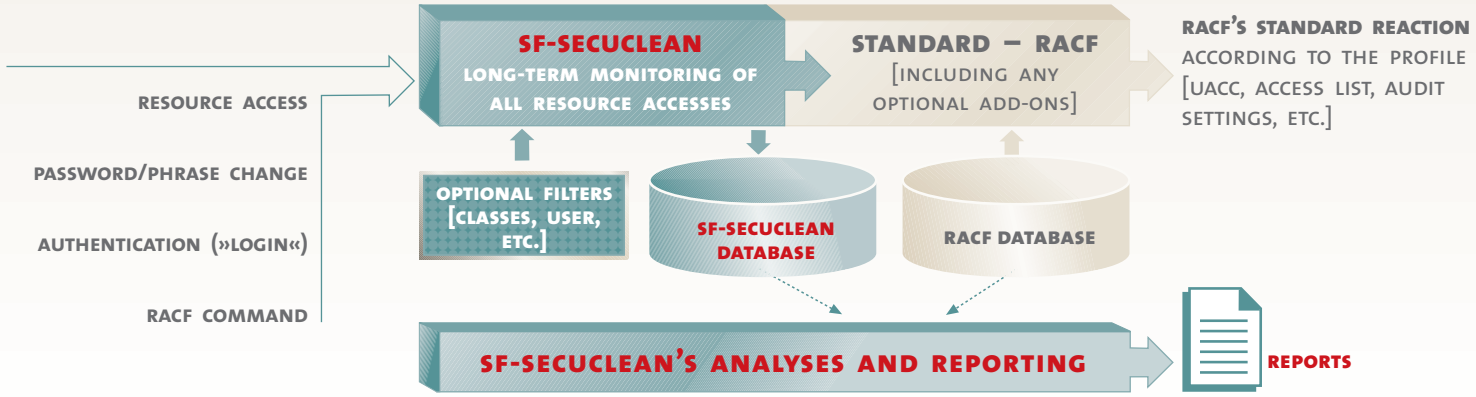
SF-SECUCLEAN'S TECHNOLOGY EXTENDS THE STANDARD RACF ENVIRONMENT WITH THE REQUIRED RESOURCE ACCESS MONITORING WITHOUT INFLUENCING RACF'S ACTUAL DECISIONS. ALL RESOURCE ACCESS REQUESTS ARE REGISTERED IN A DATABASE (DB2) THAT IS AVAILABLE FOR ONLINE EVALUATION AND REPORTING AT ANY TIME. A PRECISE KNOWLEDGE BASE IS CREATED OVER TIME REGARDING WHICH USERS (MUST) ACCESS WHICH RESOURCES ON WHICH ACCESS LEVELS FOR THEIR DAILY WORK. THE LONGER THE OBSERVATION PERIOD, THE GREATER THE INFORMATIVE VALUE OF THIS MONITORING BECOMES. IN THE END, I.E. AFTER A SUFFICIENT LENGTH OF TIME, CLARITY ARISES REGARDING EACH USER'S ACTUALLY REQUIRED AUTHORIZATIONS, WHICH THEN ALLOWS YOU TO RECONFIGURE AND OPTIMIZE THE RACF DATABASE WITH MINIMUM RISK. OF COURSE, SF-SECUCLEAN'S UNIQUE MONITORING CAPABILITIES ALSO SUPPORT DAILY WORK IN YOUR RACF ADMINISTRATION, SECURITY MONITORING, SYSTEM PROGRAMMING AND IT AUDIT DEPARTMENTS. INFORMATION REGARDING (REAL) OCCURRING ACCESS REQUESTS CAN BE OBTAINED ONLINE AT ANY TIME BY FOLLOWING A SIMPLE PROCEDURE.

SF-SECUCLEAN IS THEREFORE THE IDEAL SOLUTION FOR ALL MAINFRAME USERS ACROSS ALL BUSINESS SECTORS OR COMPANY SIZES. IT IS ALSO THE "PERFECT MATCH" FOR ALL PRAGMATIC Z/OS USERS WHO DISMISS ANY "MONITORING AND COMPLIANCE OVERKILL" AND JUST DESIRE A **STATE-OF-THE-ART CLEANUP AND HIGH-PERFORMANCE CONFIGURATION** OF THEIR RACF SECURITY WITHOUT INVESTING A LOT IN CPU TIME AND OTHER COSTS. CHECK IT OUT!

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.com

ULTIMATE EFFECTIVENESS OF RACF VIA CLEANNESS, COMPLIANCE AND PERFORMANCE

»CLEANING UP RACF HAS NEVER BEEN SO EASY AND RISK-FREE!



» What does it mean to clean up the RACF database in practice?

The following functions assist you in cleaning up the RACF database, i.e. to

- delete any unused and therefore redundant user, group and resource profiles,
- aggregate profiles expediently,
- cut unnecessary authorizations given by excessive access lists,
- **delete redundant entries from access lists,**
- remove global access authorizations,
- reorganize groups to keep access lists small, as well as to
- selectively lower the universal access (UACC) to further limit access, or
- increase the UACC to, in some cases, keep the access list (more) compact.

» What advantages are gained from cleaning up the RACF database?

First, such a cleanup provides the RACF database with a degree of transparency, relief from redundancy, and compliance required in today's IT environment. It will depict a **representative as-is state of your required authorizations that is free of the usual authorization backlogs.** Second, RACF's performance is increased while its CPU usage required for security checks is decreased. Overly extensive access lists, unused profiles, etc. result in avoidable overhead since RACF must run through these redundant structures itself every time as well. You must also consider that the volume of resource access checks performed in a productive z/OS system can easily exceed several millions a day.

» What problems and risks arise from lowering the UACC in practice?

The so-called "universal access" control of a RACF profile, abbreviated UACC, determines the general access authority to the resources protected by the profile. The UACC steps in whenever the user's authority is not determined by the profile's access list, i.e. via a corresponding user or group-related entry. Thus, in the case of a required UACC cut, the **main challenge** is to identify all users accessing relevant resources via the profile's UACC - instead of its access list. These users need to be entered in the profile's access list **before adjusting the UACC.** It is exactly in such cases that SF SecuClean provides the necessary clear answer by providing the required long-term resource access monitoring. Its comprehensive technology keeps track of all resource accesses including the details, such as user ID, access level, etc. Users accessing the resource without being authorized by the current access list need to be added in order to avoid any production problems. Standard reports provided by **SF-SecuClean** let you easily identify such required access list entries.

» Why are alternatives to SF-SecuClean's approach usually riskier, more problematic and, in the end, more cost-intensive?

To realize how practical and important this issue really is, consider how often a company's management has chosen to do without a UACC or access list cut after having thoroughly examined all the potential risks together with their specialists. The following alternative procedures are likely to be discussed while management searches for a quick and cheap solution:

a) **Analyzing the RACF SMF records:** The problem results from incompleteness of the SMF records. RACF's event logging depends on too many controls, such as the audit settings on the user, profile and class levels, for example. There are also RACF classes and authority check types that ignore any audit setting (see below). **It is therefore highly likely that the relevant SMF evaluations are incomplete.** System administrators will also be partly afraid of potential operative problems to their applications, such as extended CPU and response times in case of additionally enabled logging that causes a significant increase in SMF records.

b) **Enabling the so-called "warning mode":** By changing a profile into warning mode, all access requests not covered by the access list or the UACC are temporarily approved together with an explicit log thereof. An evaluation of the RACF SMF records tagged with "warning mode" over a corresponding length of time, will, together with ongoing access list maintenance, eventually result in the required access list. If no further access requests arise thanks to the warning mode, it can be turned off again. **What is the root of the problem and the high risk involved from an authorization cut via the "warning mode method"?** When the warning mode is activated, all users virtually receive unlimited access to all the resources protected by the profile. When these resources are files, these are also in danger of being deleted. This kind of high risk is only very hard to justify in a typical productive environment, actually only as an exception. In the worst case, warning mode profiles are completely neglected and remain a security gap for a long time.

Note that both approaches are sub-optimal and involve serious risks. However, SF-SecuClean lets you avoid these unacceptable security and operational risks by using a trouble-free and high-performance technology that completely records all resource access requests without producing SMF records or any impact on the actual process.

» Why does RACF's regular [audit] logging not result in the completeness required by such a long-term monitoring?

The potential insufficient completeness of z/OS and RACF SMF log data is a complex and extensive subject. When you need to implement complete long-term monitoring of resource accesses, **gaps in the SMF-based logging** can be due to the fact that

- RACF does not log any access requests for users with the PRIVILEGED attribute,
- nor does LOGOPTIONS(ALWAYS) result in guaranteed logging, e.g. in the case of "RACROUTE REQUEST=FASTAUTH" access checks,
- global access regulations result in a corresponding absence of logging activity,
- applications with their own resource access requests may suppress any logging, and
- RACF commands that just list and search through profiles are principally not logged.

SF-SecuClean closes this gap with truly complete logging of all your resource access requests.

» Why is long-term monitoring also a prerequisite in successfully setting up an initial role model?

The records provided by long-term monitoring are not only useful for a RACF cleanup, but are also the ideal basis for an initial role model that reflects the **as-is status of required authorizations.** Why does an initial evaluation of your required authorizations based on the RACF database only lead to less than optimal results? Without a preliminary cleanup, the RACF database is most likely to grant too far-reaching authorizations. This means, the RACF database is more or less far away from representing the "ideal" situation, where all users are authorized on a "need to have" basis. A corresponding role model would imply excessive authorizations and practically stand in the way of a real restart that is always based on a non-redundant, slim and strict authorization model.

All in all, when you **set up a role model** in the area of mainframe security, follow these steps: a) Establish long-term monitoring, and b) systematically clean up security definitions and authorities. Only then can an initial role model be derived from the "now clean" as-is state of the RACF database.

» What distinguishes our SF-SecuClean technology from other solutions?

Access to resources and relevant access checks constantly occur in a productive system because of the many processes running on it. Its high-frequent execution and deep implementation in the operating and RACF systems cause **extreme demands to such a monitoring technology.** SF-SecuClean proves its worth in terms of reliability, flexibility, performance, stability, non-interference and robustness as shown below.

» SF-SecuClean

- monitors all resource access requests, including those performed via FASTAUTH and the PRIVILEGED attribute,
- does not create additional SMF records, and thus cannot have negative effects on regular SMF processing,
- never interferes with and delays your actual applications and processes,
- never depends on the RACF audit settings on the user, profile or class levels,
- allows free choice regarding the monitored resource classes,
- keeps all results in DB2 tables for highly flexible processing, such as for SQL-based reporting,
- includes standard reports that provide answers to typical concerns,
- prevents any data loss during DB2 off-times via a secure intermediate storage,
- optimizes its processing to minimize DB2-related processing,
- supports the optional exclusion of dedicated applications, users, classes, etc.,
- supports dynamic RACF exits in case an installation has made them "dynamic,"
- represents no risk since no automatic alteration of the RACF database is performed, but recommendations result in the form of reports,
- optionally forwards results to IDM, IDS and SIEM systems,
- guarantees full automation of all its processes involved, and
- causes minimum CPU consumption thanks to highly efficient routines and optimized overall processing.

» No doubt, because of SF-SecuClean, achieving transparency, compliance and performance of the RACF database have never been easier and more efficient, and at such minimal cost. Take our word for it!