SF-LOGINHOOD®

ULTIMATE PASSWORD AND LOGIN SECURITY ON Z/OS VIA POWERFUL RACF ADD-ON

YOUR GOALS

ENSURES THE HIGHEST POSSIBLE PASSWORD AND PHRASE QUALITY EVER

COMPLETES RACF WITH NECESSARY HIGH SOPHISTICATED AND FULLY-AUTOMATED CONTROLS

ENSURES MAXIMUM PROTECTION OF ALL RACF AUTHENTICATION SERVICES AGAINST ANY MISUSE

HARDENING THE LOGIN AND PASSWORD SECURITY ON Z/OS FOR STATE-OF-THE-ART PROTECTION AND COMPLIANCE

z/OS penetration tests and audits clearly prove: **Weaknesses in password and login security lead to a particularly high vulnerability** - and quick success for the attacker. Why? First, although RACF does sport some login-related protection features and offers supplemental products, it still does **not provide sufficiently sensitive ("filigree") and automated security controls actually required in the fields of login and password security.** Second, these are usual omissions made by the mainframe user himself regarding a general lack of real-time quality assurance, monitoring and audit in the areas of user ID, password, phrase and certificates.

As a powerful, cost-effective and hardware-less solution, SF-LoginHood paves the new integral path to state-of-the-art protection of the z/OS platform in the area of password and login security. Our company's independence allowed a uniquely relentless and effective identification of all risks associated with the z platform in order to

- **guarantee maximum password and phrase quality,**
- **provide maximum protection against theft of any authentication-related data,**
- **employ additional hardening of the authentication mechanisms that prevent their abuse,**
- **ensure transparency and completeness in effectively logging 100% of all relevant activities, and to**
- **establish real-time anomaly detection on the system, administration and user levels.**

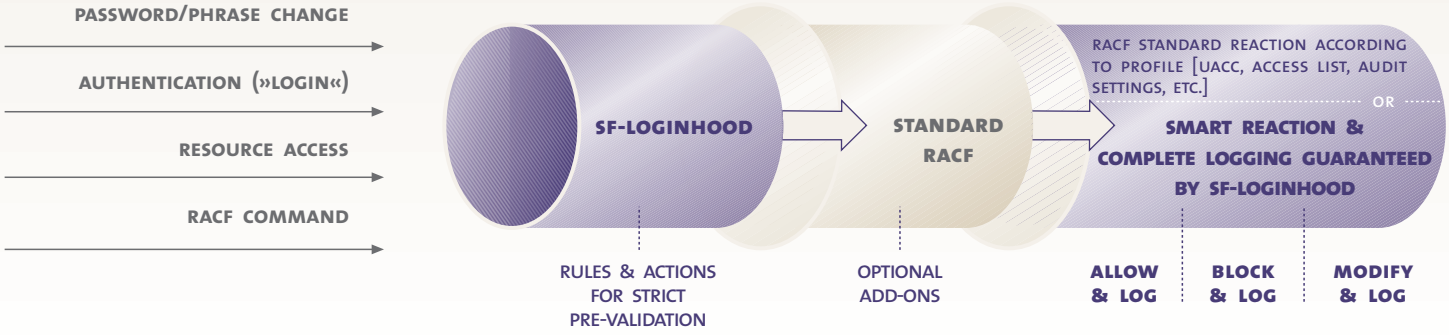
This spectrum of necessary precautionary measures in the "z entrance area" clearly proves both. Simply setting up a list of forbidden passwords is just not enough anymore. Do not forget that RACF still requires you to program an exit in Assembler to realize that measure. Merely implementing audit solutions to reveal problems "ex-post" is also too little too late.

Euro-SOX, Basel II, PCI, ISO, BSI, DOD, and other standards make additional **pro-active measures in the login environment** almost a 100% duty - not only for financial service providers - and are a prerequisite for receiving the certificate of compliance. **SF-LoginHood** was developed specifically for this purpose in a needs-based approach based on 15 years of practical experience. You can say it is an optimally aligned and overhead-free bundle of effective measures that tackles all of the above-mentioned problems at the root by completing the z/OS security based on RACF. **SF-LoginHood is therefore the ideal solution for all mainframe users across all business sectors and company sizes.** It is also the "perfect match" for all pragmatic z/OS users who dismiss any "monitoring or compliance overkill" and just desire a strong and state-of-the-art protection for their sensitive "z/OS entrance area".

Do you already use or plan to use any Smart Card, Token or Identity Management solution? That's a good idea! SF-LoginHood does not become superfluous. On the contrary, only SF-LoginHood completes these measures, and could even be a **low-cost alternative to these.** Check it out!

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.com

»FINALLY, THE Z/OS MAINFRAME BECOMES AN IMPREGNABLE FORTRESS!«



» Guaranteeing the most stringent real-time quality assurance within the context of password/phrase change or initial assignment:

- **SF-LoginHood** lets you apply password and phrase quality rules that provide capabilities going far beyond RACF's "out of the box" features. It simply becomes impossible for users and administrators to use unsafe passwords and phrases. Risks from so-called "vendor-supplied standard passwords" and "default passwords" are thereby completely eliminated.
- **Environments requiring top-level security were the reference.** All quality and security parameters relevant in best practice are supported accordingly in an "easy to use" manner, such as minimum length, compulsory character set, forbidden words, repetition of single characters or strings, and much more.
- You can define all these quality and audit rules in a transparent and audit-compliant manner. These can be altered at any time **without the typical hassles involved,** such as exit programming in Assembler, re-IPLing the system, etc.
- **Finally, you can establish individually complex rules** for different user categories. For example, you may easily allow specific users to use a minimum password length half the normal size – as an exception. Categories can be easily defined and it also supports dynamic criteria, which permits automatic or implicit classification.
- You may block particular **password changes** to achieve a 100% guarantee of risk prevention, such as for specific accounts like technical user IDs . Or, you can make such changes dependent upon additional confirmation requested by other authorities.
- The "pain" resulting from each particular quality measure and rule becomes fully transparent and quantifiable when implementing SF-LoginHood. This is elementary for an **accurate endorsement of their necessity** and significance at the user's site and lets you safely decide for a possible mitigation.

» Control, protection and monitoring of all authentication processes ("logins") as a precaution against any potential abuse of, and attacks on the RACF authentication services:

- **SF-LoginHood** lets you finally subject particularly **privileged users** to much more precise requirements than currently possible. For example, in addition to the standard restriction, such as based on time, weekday and date, SF-LoginHood supports a specific version of the four-eye principle that requires a so-called reference user to be active ("logged in") already. This lets you enjoy better control over emergency or external user IDs.
- **New authentication restrictions based on environmental parameters** let you make the z/OS login more secure. For example, the login permission for particular accounts is only given for dedicated IP addresses, applications (address spaces), a batch environment, or similar technical criteria.
- Another major problem is also solved by **SF-LoginHood: defense against login-based sabotage or corresponding attacks** on critical accounts - for example via JCL, any generally accessible mainframe applications, such as TSO, FTP, etc., or any host-connected client software. SF-LoginHood completes RACF's PROTECTED attribute concept by preventing arbitrary authentications to critical users. Only this technological measure will completely eliminate the risk of high-potential damage to your valuable system!

» Constant validation and monitoring of all authentication-relevant data and control parameters:

- **SF-LoginHood** constantly monitors **all RACF control parameters** in the areas of password, phrase, certificate and authentication regarding any change, as well as their validity and compliance.
- RACF's **"enveloped password" feature** supports the decipherable storage of passwords, i.e. their back translation into clear text. The detailed monitoring provided in this field uncovers any abuse and unintended configuration.
- Applications or subsystems maintaining **their own authentication procedures** and keeping any related data in their own databases, instead of using RACF, can be monitored accordingly.
- **Any clear text passwords** stored in procedures, scripts, or corresponding files, are disclosed via automatically performed system scans.
- **The effective password and phrase quality** is regularly assessed via a fully-automated "password cracking" applied on the RACF database. This ultimate assessment is trouble-free since it is based on a simulation, and the required **CPU load may be delegated to zIIP processors,** if any are available.

» All affected activities are recorded transparently and gap-less so that legal requirements and software-based detection procedures can unfold their full effectiveness:

- **SF-LoginHood** provides RACF with the required **log-related completeness** concerning successful and unsuccessful logins, password changes, etc. Finally, **100% transparency** is ensured in the area of authentication because SF-LoginHood guarantees to record all events with any and all details.
- An **easy integration** into your existing log recording and archiving procedures is given since SMF records are used.
- It is generally difficult to doubt the completeness of log files especially when these already involve millions of records. Nevertheless, you must watch out for potentially missing or insufficiently logged events on the z/OS platform as well. Not only will your **auditors** but all **intrusion detection and SIEM systems** as well be grateful for the new log quality achieved by **SF-LoginHood.** If any legal concerns happen to arise, a variety of **anonymization** options will suppress any conflict of interest while fully preserving their technical usability.
- Accordingly, all administrative activities, including the areas of **revoking and resuming user IDs, and the password reset in particular,** are not only logged in real-time but also **validated** and maybe even **blocked** to promptly detect the subtlest anomalies, "malicious tricks", and potential abuse, and also to avoid potential problems in production. Only this can prevent a help-desk, for example, from getting "hold of" an account outside its actual area of responsibility despite its often too far-ranging authorities in RACF.
- **Users** can be informed **directly** and **automatically** about any anomalies regarding their own account, for example by e-mail.

» Last but not least - Preventing all worst case scenarios:

- **SF-LoginHood** establishes additional and particularly **highly subtle access blockades** that go far beyond RACF's regular access list checking. These serve to constantly monitor both granted access authorities and effective accesses to authentication and log-relevant data sets, such as the RACF database. **Your clear objective is to prevent any potential theft of this extremely sensitive data "at any cost."**
- **SF-LoginHood's** ultimate z/OS security monitoring also covers the **"tip of the risk iceberg"** which involves the (complete) bypass of the security system by performing **privilege theft** and penetrating the **audit trail** in order to freely access any data without any logging. Attackers thereby take advantage of subtle weaknesses in the z/OS system and third-party software, or any existing malicious code, to perform the corresponding manipulations using system-specific tricks.

» Without a doubt, SF-LoginHood represents the successful implementation of a 360-degree approach that allows constant and fully-automated monitoring in the areas of password and login security. Without any technical exaggeration, the z-platform's "entrance area" receives the attention and supervision so necessary in today's environment. Supported by this profound know-how in virtual form and drawing from over 15 years of practical experience, password and login security on the z/OS mainframe has never been more powerful and so cost-effective at the same time. Take our word for it!