TrashPW - Trash GUARDIAN Password

Version 400

13Nov2018

To control functional users it is necessary, to

- Individualize and control access to functional users such as APPL.MANAGER, SUPER.SUPER etc.
- Prohibit the logon to functional users via passwords 'from scratch'
- Enforce the use of command level security type controls

To really prevent the logon to a user, the password of that user has to be trashed, not simply changed. A password change, performed by a human, always has the disadvantage that the changing person might remember the password it typed in.

TrashPW solves this dilemma:

- TrashPW really trashes the password of a given GUARDIAN or Alias user ID.
- TrashPW relies on SAFEGUARD and uses the SPI interface.

The logic is this:

1. SUPER.SUPER can trash the password of
    a. any GUARDIAN user (including himself)
    b. any Alias user
2. The user's primary owner can trash a user's password.
3. Any user can trash his password.

To prevent an easy trash, TrashPW asks the user two times if he really wants to trash a password.

Once a password is trashed, there is NO WAY to logon to that user by using a password.

Technical insights:
TrashPW relies in SAFEGUARD. It uses the SPI interface to find out, if the TrashPW-user is the primary owner of the user, whose password has to be trashed. In case he is not, TrashPW aborts the session.

In another call to SAFEGUARD it gets the maximum password length, which is in the range of 8 to 64.

A 64 byte binary password is generated, and truncated to the maximum possible length. Because the generated password consists of random binary bytes, there is a very rare chance that the 'new' password is in the users password stack.
This new password is introduced to the user by another SPI call to SAFEGUARD.

Security settings:

The security vector should be: "OOAO"
The program does NOT need to become licensed.

Trashing SUPER.SUPER:

Only trash the SUPER.SUPER password when
- SECOM is installed, and ready to be used
- LASTAID is available, and ready to be used (talk to GreenHouse)

Recovery:

To recover the trashed password of a user, logon to the user's primary owner, and change the password with SAFECOM, e.g.:

```
SAFECOM ALTER USER|ALIAS <user>, PASSWORD <password>
```

In case SAFEGUARD is not running, get access to SUPER.SUPER through SECOM or LastAid, and use the PASSWORD program, e.g.:

```
$SYSTEM SUPER 6> password
USER ID: 126,37
NEW PASSWORD:
RE-ENTER NEW PASSWORD:
THE PASSWORD FOR USER (126,037) HAS BEEN CHANGED.
$SYSTEM SUPER 7>
```

In case of any question, please feel free to contact us at:

GreenHouse Software & Consulting
Carl Weber
Heinrichstrasse 12
D-45711 Datteln
Phone 49 2363 72566
FAX +49 2363 66106
E-Mail Carl.Weber@GreenHouse.de