The tcfs 2.0.1 module

1) Synopsis

Module name: pam_tcfs

Author: Luigi Catuogno [luicat@mikonos.dia.unisa.it]

Maintainer: author

Management groups provided: authentication, session, password

System dependencies: The system must be a tcfs 2.0 server/client and the sources of tcfs must be available.

2) Overview of module

This module does needed adjustments and settings to the tcsf structures/files during authentication, session, and pwd changing, according to requests and data provided by the application and by the other modules in the same pam service. The tcfs module does not perform any effective authentication. It assumes the authentication has been already done elsewere and simply decides either to activate tcfs features to registered users or not.

3) Authentication component

recognized arguments: none

description: this component of the module verifies if the user is registered to tcfs, and in this case it extracts his default tcfs-key from /etc/tcfspasswd, decrypts it with the user's auth. token and, finally, stores it in a pam-data "variable" named tcfskey, to be used by other components/modules.

example/suggested usage: since this component does not perform any conversation, it must be used together with another one which does. Whenever the module is loaded for some service, the component must be configured as "optional" because it returns PAM_SUCCESS only if the user is registered with tcfs. If the component is configured as required, access to the service would be denied to users not registered with tcfs.

4) Session component

recognized argument: none

description: If the pam-data tcfskey was previously defined, the session component pushes it into the tcfs device's hash table, in order to enable the encrypted file system owned by the user. When the session ends, it simply removes the key from the table.

examples/suggested usage: Whenever the module is loaded for services available both to tcfs users and non-tcfs users, the session component must be configured as "optional" because it returns PAM_SUCCESS only if the user is registered to tcfs (i.e., tcfskey is defined).

5) Password component

recognized arguments: none

description: since the user’s password is used to encrypt the tcfskey into /etc/tcfspasswd, whenever the token changes, the coding of the tcfs-key must consequently change. The password component extracts the key entry from the file, decodes it with the old token, encodes it with the new one, then writea it back to /etc/tcfspasswd. If the user is not registered, no changes are made.

examples/suggested usage: Since this component does not perform any conversation, it must be used together with another one which does it; furthermore it must be configured as "required" for each service it is included, in order to save the validity of tcfskey extracted from /etc/tcfspasswd during authentications.