NAME

pam_xauth - PAM module to forward xauth keys between users

SYNOPSIS

pam_xauth.so [debug] [xauthpath=*/path/to/xauth*] [systemuser=*UID*] [targetuser=*UID*]

DESCRIPTION

The pam_xauth PAM module is designed to forward xauth keys (sometimes referred to as "cookies") between users.

Without pam_xauth, when xauth is enabled and a user uses the **su(1)** command to assume another user's privileges, that user is no longer able to access the original user's X display because the new user does not have the key needed to access the display. pam_xauth solves the problem by forwarding the key from the user running su (the source user) to the user whose identity the source user is assuming (the target user) when the session is created, and destroying the key when the session is torn down.

This means, for example, that when you run **su(1)** from an xterm session, you will be able to run X programs without explicitly dealing with the **xauth(1)** xauth command or ˜/.Xauthority files.

pam_xauth will only forward keys if xauth can list a key connected to the $DISPLAY environment variable.

Primitive access control is provided by ˜/.xauth/export in the invoking user's home directory and ˜/.xauth/import in the target user's home directory.

If a user has a ˜/.xauth/import file, the user will only receive cookies from users listed in the file. If there is no ˜/.xauth/import file, the user will accept cookies from any other user.

If a user has a .xauth/export file, the user will only forward cookies to users listed in the file. If there is no ˜/.xauth/export file, and the invoking user is not **root**, the user will forward cookies to any other user. If there is no ˜/.xauth/export file, and the invoking user is **root**, the user will *not* forward cookies to other users.

Both the import and export files support wildcards (such as *). Both the import and export files can be empty, signifying that no users are allowed.

OPTIONS

debug

Print debug information.

xauthpath=*/path/to/xauth*

Specify the path the xauth program (it is expected in /usr/X11R6/bin/xauth, /usr/bin/xauth, or /usr/bin/X11/xauth by default).

systemuser=*UID*

Specify the highest UID which will be assumed to belong to a "system" user. pam_xauth will refuse to forward credentials to users with UID less than or equal to this number, except for root and the "targetuser", if specified.

targetuser=*UID*

Specify a single target UID which is exempt from the systemuser check.

MODULE TYPES PROVIDED

Only the **session** type is provided.

RETURN VALUES

PAM_BUF_ERR

Memory buffer error.

PAM_PERM_DENIED

Permission denied by import/export file.

PAM_SESSION_ERR

Cannot determine user name, UID or access users home directory.

PAM_SUCCESS

Success.

PAM_USER_UNKNOWN
   User not known.

EXAMPLES

Add the following line to /etc/pam.d/su to forward xauth keys between users when calling su:

session optional pam_xauth.so

IMPLEMENTATION DETAILS

pam_xauth will work *only* if it is used from a setuid application in which the **getuid**() call returns the id of the user running the application, and for which PAM can supply the name of the account that the user is attempting to assume. The typical application of this type is **su(1)**. The application must call both **pam_open_session**() and **pam_close_session**() with the ruid set to the uid of the calling user and the euid set to root, and must have provided as the PAM_USER item the name of the target user.

pam_xauth calls **xauth(1)** as the source user to extract the key for $DISPLAY, then calls xauth as the target user to merge the key into the a temporary database and later remove the database.

pam_xauth cannot be told to not remove the keys when the session is closed.

FILES

˜/.xauth/import
   XXX

˜/.xauth/export
   XXX

SEE ALSO

pam.conf(5), **pam.d(5)**, **pam(7)**

AUTHOR

pam_xauth was written by Nalin Dahyabhai <nalin@redhat.com>, based on original version by Michael K. Johnson <johnsonm@redhat.com>.