NAME

pam_u2f − Module for U2F authentication

SYNOPSIS

pam_u2f [...]

DESCRIPTION

The module provides U2F authentication against Yubikeys and other compliant authenticators.

OPTIONS

debug

Enables debug output

debug_file

Filename to write debugging messages to. **If this file is missing, nothing will be logged**. This regular file **has to be created by the user** or **must exist and be a regular file** for anything getting logged to it. It is not created by pam−u2f on purpose (for security considerations). This filename may be alternatively set to "stderr" (default), "stdout", or "syslog".

origin=*origin*

Set the relying party ID for the FIDO authentication procedure. If no value is specified, the identifier "pam://$HOSTNAME" is used.

appid=*appid*

Set the application ID for the U2F authentication procedure. If no value is specified, the same value used for origin is taken ("pam://$HOSTNAME" if also origin is not specified). This setting is only applicable for U2F credentials created with pamu2fcfg versions v1.0.8 or earlier. Note that on v1.1.0 and v1.1.1 of pam−u2f, handling of this setting was temporarily broken if the value was not the same as the value of origin.

authfile=*file*

Set the location of the file that holds the mappings of user names to keyHandles and user keys. An individual (per user) file may be configured relative to the users' home dirs, e.g. ".ssh/u2f_keys". If not specified, the location defaults to $XDG_CONFIG_HOME/Yubico/u2f_keys. If $XDG_CONFIG_HOME is not set, $HOME/.config/Yubico/u2f_keys is used. The authfile format is <username>:<KeyHandle1>,<UserKey1>,<CoseType1>,<Options1>:<KeyHandle2>,<UserKey2>,<CoseType2>,<C

authpending_file=*file*

Set the location of the file that is used for touch request notifications. This file will be opened when pam−u2f starts waiting for a user to touch the device, and will be closed when it no longer waits for a touch. Use inotify to listen on these events, or a more high−level tool like yubikey−touch−detector. Default value: /var/run/user/$UID/pam−u2f−authpending. Set an empty value in order to disable this functionality, like so: "authpending_file=".

nouserok

Set to enable authentication attempts to succeed even if the user trying to authenticate is not found inside authfile or if authfile is missing/malformed.

openasuser

Setuid to the authenticating user when opening the authfile. Useful when the user’s home is stored on an NFS volume mounted with the root_squash option (which maps root to nobody which will not be able to read the file). Note that after release 1.0.8 this is done by default when no global authfile or XDG_CONFIG_HOME environment variable has been set.

alwaysok

Set to enable all authentication attempts to succeed (aka presentation mode).

max_devices=*n_devices*

Maximum number of devices allowed per user (default is 24). Devices specified in the authentication file that exceed this value will be ignored.

interactive

Set to prompt a message and wait before testing the presence of a U2F device. Recommended if your device doesn’t have tactile trigger.

[prompt=your prompt here]
Set individual prompt message for interactive mode. Watch the square brackets around this parameter to get spaces correctly recognized by PAM.

manual
Set to drop to a manual console where challenges are printed on screen and response read from standard input. Useful for debugging and SSH sessions without U2F−support from the SSH client/server. If enabled, interactive mode becomes redundant and has no effect.

cue
Set to prompt a message to remind to touch the device.

[cue_prompt=your prompt here]
Set individual prompt message for the cue option. Watch the square brackets around this parameter to get spaces correctly recognized by PAM.

nodetect
Skip detecting if a suitable key is inserted before performing a full authentication. See **NOTES** below.

userpresence=*int*
If 1, require user presence during authentication. If 0, do not request user presence during authentication. If omitted, fallback to the authenticator’s default behaviour.

userverification=*int*
If 1, require user verification during authentication (e.g. biometrics). If 0, do not request user verification during authentication. If omitted, fallback to the authenticator’s default behaviour. If enabled, an authenticator with support for FIDO2 user verification is required.

pinverification=*int*
If 1, require PIN verification during authentication. If 0, do not request PIN verification during authentication. If omitted, fallback to the authenticator’s default behaviour. If enabled, an authenticator with support for a FIDO2 PIN is required.

sshformat
Use credentials produced by versions of OpenSSH that have support for FIDO devices. It is not possible to mix native credentials and SSH credentials. Once this option is enabled all credentials will be parsed as SSH.

EXAMPLES

auth sufficient pam_u2f.so debug origin=pam://$HOSTNAME appid=pam://$HOSTNAME

auth required pam_u2f.so origin=http://example.com appid=http://example.com
authfile=/etc/yubikey_mappings

CAVEATS

By default the mapping file inside a home directory will be opened as the target user, whereas the central file will be opened as "root". If the "XDG_CONFIG_HOME" variable is set, privileges will not be dropped unless the "openasuser" configuration setting is set.

Using pam−u2f to secure the login to a computer while storing the mapping file in an encrypted home directory, will result in the impossibility of logging into the system. The partition is decrypted after login and the mapping file can not be accessed.

NOTES

Nodetect

The "nodetect" option should be used with caution. pam_u2f checks that a key configured for the user is inserted before performing the full tactile authentication. This detection is done by sending a "check−only" authentication request to all inserted tokens to so see if at least one of them responds affirmatively to one or more of the keyhandles configured for the user. By doing this, pam_u2f can avoid emitting the "cue" prompt (if configured), which can cause some confusing UI issues if the cue is emitted followed by the underlying library immediately failing the tactile authentication. This option is also useful to avoid an unintended 1−second delay prior to the tactile authentication caused by versions of libu2f−host <= 1.1.5.

If pam_u2f is configured to "cue" and "nodetect", an attacker can determine that pam_u2f is part of the authentication stack by inserting any random U2F token and performing an authentication attempt. In this scenario, the attacker would see the cue message followed by an immediate failure, whereas with detection enabled, the U2F authentication will fail silently. Understand that an attacker could choose a U2F token that alerts him or her in some way to the "check−only" authentication attempt, so this precaution only pushes the issue back a step.

In summary, the detection feature was added to avoid confusing UI issues and to prevent leaking information about the authentication stack in very specific scenario when "cue" is configured. The "nodetect" option was added to avoid buggy sleep behavior in older versions of libu2f−host and for hypothetical tokens that do not tolerate the double authentication. Detection is performed, and likewise "nodetect" honored, regardless of whether "cue" is also specified.

SELinux

Due to an issue with Fedora Linux, and possibly with other distributions that use SELinux, a system configured with pam−u2f may end up in a situation where access to the credentials file is denied. If the nouserok option is also set, this will result in a successful authentication within the module, without using the FIDO authenticator.

In order to correctly update the security context the command **fixfiles onboot** should be used on existing installations

Moreover, to allow read access to an authfile or directory placed in a non−standard location, the command

```
# chcon −R −t auth_home_t /path/to/authfile
```

should be used.

For more information see https://access.redhat.com/security/cve/CVE−2020−24612.

BUGS

Report pam−u2f bugs in the issue tracker: https://github.com/Yubico/pam−u2f/issues

SEE ALSO

pam(7)

The pam−u2f home page: https://developers.yubico.com/pam−u2f/

YubiKeys can be obtained from Yubico: http://www.yubico.com/