NAME

ykpamcfg − Manage user settings for the Yubico PAM module

SYNOPSIS

ykmapcfg [−1 | −2] [−A] [−p] [−i] [−v] [−V] [−h]

OPTIONS

−1
use slot 1. This is the default.

−2
use slot 2.

−A *action*
choose action to perform. See ACTIONS below.

−p *path*
specify output file, default is ˜/.yubico/challenge

−i *iterations*
number of iterations to use for pbkdf2 of expected response

−v
enable verbose mode.

−V
display version and exit

−h
display help and exit

ACTIONS

add_hmac_chalresp

The PAM module can utilize the HMAC−SHA1 Challenge−Response mode found in YubiKeys starting with version 2.2 for **offline authentication**. This action creates the initial state information with the C/R to be issued at the next logon.

The utility currently outputs the state information to a file in the current user's home directory (*˜/.yubico/challenge−123456* for a YubiKey with serial number API readout enabled, and *˜/.yubico/challenge* for one without).

The PAM module supports a system wide directory for these state files (in case the user's home directories are encrypted), but in a system wide directory, the *challenge* part should be replaced with the username. Example : */var/yubico/challenges/alice−123456*.

To use the system−wide mode, you currently have to move the generated state files manually and configure the PAM module accordingly.

EXAMPLES

First, program a YubiKey for challenge response on Slot 2 :

```
$ ykpersonalize −2 −ochal−resp −ochal−hmac −ohmac−lt64 −oserial−api−visible
...
Commit? (y/n) [n]: y
```

Now, set the current user to require this YubiKey for logon :

```
$ ykpamcfg −2 −v
...
Stored initial challenge and expected response in '/home/alice/.yubico/challenge−123456'.
```

Then, configure authentication with PAM for example like this (*make a backup first*) :

/etc/pam.d/common−auth (from Ubuntu 10.10) :

```
auth  required       pam_unix.so nullok_secure try_first_pass
auth  [success=1 new_authtok_reqd=ok ignore=ignore default=die] pam_yubico.so mode=challenge−response
auth  requisite      pam_deny.so
auth  required       pam_permit.so
auth  optional       pam_ecryptfs.so unwrap
```

BUGS

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

SEE ALSO

pam_yubico(8)

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

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