====== PAM mit U2F Auth (Hardware Dongle)

Using U2F at Linux Login

Setup PAM

Linux uses PAM (Pluggable Authentication Modules) to handle all authentication tasks. Since I am going to modify how I login (authenticate) to the system, using FIDO U2F, I need a PAM module providing this functionality.

```
$ apt-cache libpam-u2f
libpam-u2f:
  Installed: (none)
  Candidate: 1.0.4-2
  Version table:
     1.0.4-2 500
        500 http://de.archive.ubuntu.com/ubuntu bionic/universe amd64
Packages
```

Register a U2F Token

I will use the pamu2fcfg tool that is built together with pam_u2f.so above. I run this with the same user, so I omit -u, and I explicitly specify the origin and appid rather than using the default ones, so:

```
$ pamu2fcfg -opam://mydesktop -ipam://mydesktop
</bash>

This will output a configuration line which I need and after running this
the U2F device will blink and I touch it to complete the registration. I
actually redirect it directly to the config file:
<code bash>
$ cd ~
$ mkdir .config/Yubico
$ pamu2fcfg -opam://mydesktop -ipam://mydesktop > .config/Yubico/u2f_keys
```

This path is the default path pam_u2f.so will look for each user.

Configure PAM

I add the following line to the end of /etc/pam.d/common-auth:

```
auth sufficient pam_u2f.so debug cue nouserok origin=pam://mydesktop
appid=pam://mydesktop
```

Since I set the origin and appid when using pamu2fcfg, I also use origin and appid parameters here.

This configuration will make use of U2F device, if $HOME/.config/Yubico/u2f_keys file is present, and if it is not present (or invalid) authentication will succeed (nouserok parameter). If you use the 1.0.4 version, this is not going to work, so make sure you use the latest version of pam_u2f. Parameter cue prompts a message to remind to touch U2F device.

Very Important: The u2f_keys file should not be under an encrypted file system, because files can be decrypted only after a successful authentication which requires u2f_keys file.

It is also possible to use a single system wide configuration (single u2f_keys file) rather than using per-user u2f_keys file using the authfile parameter of pam_u2f.

Go Live

As everything is working as expected, I modify the U2F config in common-auth and change sufficient to required and remove the debug parameter.

```
auth required pam_u2f.so cue nouserok origin=pam://mydesktop
appid=pam://mydesktop
```

Since it is “required” now, pam_u2f will succeed when:

- there is no U2F registration (no u2f_keys file) for the user trying to authenticate (nouserok parameter).
- there is a U2F registration given under $HOME/.config/Yubico/u2f_keys of the user trying to authenticate and U2F device is plugged, touched and U2F authentication process completes successfully.