Yubico PAM module

The Yubico PAM module provides an easy way to integrate the Yubikey into your existing user authentication infrastructure. PAM is used by GNU/Linux, Solaris and Mac OS X for user authentication, and by other specialized applications such as NCSA MyProxy.

1. Status and Roadmap

The module is working for single-user systems.

Several items have been identified that needs to be implemented before it can reach production quality:

- Verification of server signature
- Generating signature on request
- HTTPS support
- Multi-user mappings from Yubikey to username.

The development community is co-ordinated via Google Code:

`http://code.google.com/p/yubico-pam/`

The license for pam_yubico is the same as for Linux-PAM, namely a dual-license between 3-clause BSD and the GPL. See the file COPYING for more information.

2. Building from SVN

Skip to the next section if you are using an official packaged version.

You may check out the sources using SVN with the following command:

```
svn checkout http://yubico-pam.googlecode.com/svn/trunk/ yubico-pam
```

This will create a directory *yubico-pam*. Enter the directory:

```
cd yubico-pam
```

Autoconf and automake must be installed. For the documentation, asciidoc and docbook are also required.

Generate the build system using:

```
autoreconf --install
```

3. Building

You will need to have libcurl (curl.h, libcurl.so) and libpam-dev (security/pam_appl.h, libpam.so) installed.

The build system uses Autoconf, to set up the build system run:

```
./configure
```

Then build the code, run the self-test and install the binaries:

```
make check install
```

4. Configuration

Install it in your PAM setup by adding a line to an appropriate file in /etc/pam.d/:

```
auth sufficient pam_yubico.so id=16 debug
```

and create a symlink for pam_yubico.so in /lib/security/:

```
ln -s /usr/local/lib/security/pam_yubico.so /lib/security/
```

Supported PAM module parameters are:

```
"id":       to indicate your client identity,
"debug":    to enable debug output to stdout,
"alwaysok": to enable that all authentication attempts should succeed
            (aka presentation mode).
"url":      specify URL to use for verification, by default it is
            "http://api.yubico.com/wsapi/verify?id=%d&otp=%s"
            Be sure to have only two printf tokens in the string
            and that %d comes before %s.  The %d will be replaced
            with the "id" value and %s with the user's OTP.
```

If you are using "debug" you may find it useful to create a world-writable log file:

```
touch /var/run/pam-debug.log
chmod go+w /var/run/pam-debug.log
```

5. Feedback

If you want to discuss anything related to the Yubico PAM module, please contact Simon Josefsson (mailto:simon@yubico.com).

6. Legal